NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PUBLIC SAFETY COMMUNICATIONS CENTERS: ARE WE PREPARED FOR THE NEW TECHNOLOGIES COMING OUR WAY?

by

Marc R. Shaw

March 2014

Thesis Advisor: Lauren Wollman
Second Reader: Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
PUBLIC SAFETY COMMUNICATIONS CENTERS: ARE WE PREPARED FOR THE NEW TECHNOLOGIES COMING OUR WAY?

5. FUNDING NUMBERS

6. AUTHOR(S) Marc R. Shaw

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis explores the impact of rapidly evolving emerging technologies on public safety communications centers. It is intended to further the discussion on whether the public safety community is prepared for these new technologies, which will likely become commonplace over the next several years, and how to prepare to integrate those technologies into existing structures. Through the use of a nominal group technique and cross-impact analysis, this thesis utilized a pre-collected data set concerning the risks, structure, governance, policy and external influences associated with public safety communications centers in light of emerging technological advancements to determine what trends and events were of the greatest concerns to those actively involved in the leadership of public safety communications centers, development of emerging technologies, and implementation of governance models used by the various agencies. Those findings were analyzed and strategies were identified to allow for successful mitigation of the most statistically significant risks. Ultimately, this thesis determined that through visionary leadership, effective strategic planning and mitigation of risk, public safety agencies could position themselves for successful implementation of emerging technologies with their communications centers.

14. SUBJECT TERMS Public Safety, Communications Center, Cloud, Emerging Technology	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PUBLIC SAFETY COMMUNICATIONS CENTERS—ARE WE PREPARED FOR THE NEW TECHNOLOGIES COMING OUR WAY?

Marc R. Shaw
Assistant Chief, California Highway Patrol, Glendale, CA
B.S., Saint Mary's College of California, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2014**

Author: Marc R. Shaw

Approved by: Lauren Wollman
Thesis Advisor

Richard Bergin
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the impact of rapidly evolving emerging technologies on public safety communications centers. It is intended to further the discussion on whether the public safety community is prepared for these new technologies, which will likely become commonplace over the next several years, and how to prepare to integrate those technologies into existing structures. Through the use of a nominal group technique and cross-impact analysis, this thesis utilized a pre-collected data set concerning the risks, structure, governance, policy and external influences associated with public safety communications centers in light of emerging technological advancements to determine what trends and events were of the greatest concerns to those actively involved in the leadership of public safety communications centers, development of emerging technologies, and implementation of governance models used by the various agencies. Those findings were analyzed and strategies were identified to allow for successful mitigation of the most statistically significant risks. Ultimately, this thesis determined that through visionary leadership, effective strategic planning and mitigation of risk, public safety agencies could position themselves for successful implementation of emerging technologies with their communications centers.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM SPACE....1
B. RESEARCH QUESTION....4
C. METHOD....4
D. THEORETICAL SENSITIVITY....6
E. LITERATURE REVIEW....7
F. DEFINITION OF TERMS....14
G. REVIEW OF UPCOMING CHAPTERS....23

II. DATA COLLECTION AND ANALYSIS....25
A. NOMINAL GROUP TECHNIQUE....25
B. TRENDS....26
C. EVENTS....34
D. CIA #1....41

III. ANALYSIS OF KEY ISSUES....45
A. CIA #2....46
B. COMPARISON OF CROSS IMPACT ANALYSES....47

IV. DISCUSSION....55
A. FINDINGS....55
B. IMPLEMENTATION....57
C. EVALUATION....73

V. CONCLUSION....77
A. SUMMARY....77
B. RECOMMENDATIONS....78
C. OPPORTUNITIES FOR FUTURE RESEARCH....79

APPENDIX A. TREND LISTING....81

APPENDIX B. EVENT LISTING....83

LIST OF REFERENCES....85

INITIAL DISTRIBUTION LIST....89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Overview of Emergency (9-1-1) Call Flow Today 17
Figure 2. Overview of Next Generation 9-1-1 Call Flow 21
Figure 3. Trend Analysis Graph—Level of Impact 32
Figure 4. Trend Analysis Table—Level of Concern 33
Figure 5. Event Analysis Graph—Probability Projection 39
Figure 6. Event Analysis Graph—Level of Impact 40
Figure 7. Comparison of 2011 and 2014 CIA Significance Ratings 48

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Sample Trends—Level of Impact and Concern....27
Table 2. Trend Summary Table....28
Table 3. Trends Analysis Table—Level of Impact....31
Table 4. Trends Analysis Table—Level of Concern....33
Table 5. Sample Event – Probability Projection and Level of Impact....34
Table 6. Event Summary Table....35
Table 7. Events Analysis Table—Probability Projection....38
Table 8. Events Analysis Table—Level of Impact....40
Table 9. 2011 CIA Significance Rating Table....42
Table 10. Trends Analysis Table....46
Table 11. 2014 CIA Significance Rating Table....47
Table 12. Commitment Planning Chart....70
Table 13. List of Key Stakeholders....73
Table 14. Strategic Plan Outcome Objectives....74

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALI	automatic location identification
ANI	automatic number identification
CAD	computer-aided dispatch
CAMA	centralized automatic message accounting
CHDS	Center for Homeland Defense and Security ()
CIA	cross impact analysis
CO	central office
COTS	commercial off-the-shelf
DOJ	Department of Justice
E9-1-1	enhanced 9-1-1
EOD	explosive ordnance detection
ESI Net	emergency services Internet protocol network
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
GIS	geographical information systems
GPS	global positioning system
IAAS	Infrastructure as a service
IP	Internet protocol
IT	information technology
JAB	joint authorization board
MOU	memorandum of understanding
NENA	National Emergency Number Association
NG9-1-1	next generation of 9-1-1
NGT	nominal group technique
NIST	National Institute of Standards and Technology
NSA	National Security Administration
OMB	Office of Management and Budget
PAAS	platforms as a service
PBX	public branch exchange
PIN	personal identification numbers
PSAP	public safety answering point

RoIP	radio over Internet protocol
SS7	Signaling System 7
SWAT	Special Weapons and Tactics
SWOC	strengths, weaknesses, opportunities and challenges
U.S.	United States
USDOT	United States Department of Transportation
VoIP	voice-over-Internet-protocol

ACKNOWLEDGMENTS

I am forever indebted to my wonderful wife, Carrie. Throughout this voyage (and many others), you have been by my side, always providing your love, support, and encouragement. Even when I was not sure I could continue, you always had the right words to keep me making forward progress. While I was away, you managed to maintain normalcy in our exceptionally busy lives. When I was home and struggling to meet a school deadline, you took the kids and provided peace and quiet so I could focus on my studies. I love you and appreciate you more than you will ever know. This would not have been possible without you—THANK YOU!

To my amazing children, Zac and Lily, you were always understanding on those weekend days when I said, "daddy has to do homework." For the most part, I really meant it—except maybe when you wanted to go shopping. I am excited that I will not miss any more Boy Scout events, theatre shows, softball games, or Girl Scout meetings. Thank you for not driving mommy crazy while I was out of commission.

I am grateful to my mom and dad, who raised me to work hard and achieve success in all aspects of life. This endeavor put a strain on my family, but you both graciously stepped in to help out when I was attending classes. Even if it was something simple like picking up the kids after school to spend the afternoon with them, it made a difference, and for that, I am so fortunate.

Finally, thank you to the California Highway Patrol, and specifically, Deputy Commissioner Ramona Prieto for her unwavering support and encouragement of advanced education. As someone who has never taken no for an answer, but rather as a challenge, she constantly demonstrates the traits of a true survivor. Similarly, to Dan, Bill and Sherrell, thank you for picking up the slack in my absence, and for listening to me babble about technology and all my amazing experiences throughout the past 20 months.

Although the academic rigor gained in this program was beneficial in developing my mind, the most valuable part of my life at the Center for Homeland Defense and Security is the people. The instructors are second to none and my classmates are

exceptional. I appreciate you trusting me to serve as your class president and for allowing me to represent you during the good times and the tough times. Not only did I forge friendships and professional relationships that will last for many years to come, I learned how to accept varying opinions and differing views. For that, I am a better person, a better leader, and most importantly, a better husband and father. I thank each of you for helping me achieve and realize that.

I. INTRODUCTION

A. PROBLEM SPACE

Public safety communications centers are the lifeline between emergency responders and the public. Over the past 30 years, the country has seen tremendous improvements in reliability and efficiency as technology has improved, creating vast new opportunities. However, in order to keep up with the latest technologies, public safety agencies expend an inordinate amount of personnel resources and funding. This poses a tremendous challenge for many agencies, especially smaller departments, as they already struggle with strapped budgets and diminishing resources. Public safety agencies must always be looking for a more efficient way of accomplishing their mission, while being prudent with the diminishing number of public dollars with which they have to operate.

Directors of communications centers throughout the country spend a significant amount of time, money and staff on the acquisition, implementation and maintenance of technology that is housed within their physical structure. Every function that occurs within an emergency communications center requires an investment of capital in some type of technology. Furthermore, each of those technologies requires ongoing maintenance to ensure it functions properly and securely. The normal life span of that equipment is approximately five years; yet, it may become obsolete in 18–24 months.

Trends in telecommunications mobility and technology convergence, and the growing market penetration of both cellular and Voice-over-Internet-Protocol (VoIP) telephony have underscored the limitations of the current 9-1-1 infrastructure. The nation's 9-1-1 system, now based on decades-old technology, cannot handle the applications that are increasingly common in personal communications and critical to future public safety advances. Although the 9-1-1 system has served us well for many years, the current architecture is becoming outdated as new technologies become commonplace. New forms of communication, such as text messaging, are not supported by the current 9-1-1 system. Due to these changes in technologies, the United States Department of Transportation (USDOT) and the National Emergency Number

Association (NENA) began looking at technologies to provide the platform for the next generation of 9-1-1 (NG9-1-1).

Currently, the capital outlay required to construct a communications center is tremendous. Oftentimes, before construction is complete, the equipment housed in the computer room is outdated and in need of replacement or upgrading. However, with the advent of the "cloud" the opportunities for consolidating resources and saving money have increased exponentially. Concepts like Infrastructure as a Service and Platforms as a Service allow agencies to move the information technology responsibilities outside of their department to companies that specialize in that line of work.[1] This affords them the ability to focus on their core mission—public safety. The potential paradigm shift in the business model of traditional communications centers would be drastically altered with a change, such as this, however, that means the possible improvements to the process are infinite.

Although there is documentation showing the federal government supports movement to cloud-based platforms, there are certainly concerns regarding information stored there. Initially, many public safety agency directors felt physical control of their data was a necessity, meaning data servers must be at a secure location, such as their police station. The public sector, though, has embraced the need for secure cloud space and created specific segments that meet the standards contained in the Federal Information Security Management Act, such as Google Apps for Government, which provides segregated systems for United States government customers and for which the data are stored exclusively in the United States. As cloud technologies have become more common, the public sector has exponentially increased its investment and created secure data centers designed to host public safety cloud solutions.

The potential opportunities of migrating to a cloud-based environment do not come without a host of questions and concerns. Some of these include third party access to the system, which potentially provides a security vulnerability; lack of existing private cloud infrastructure in local agencies/government and the high cost of initial architecture,

[1] Gary Garrison, Sanghyun Kim, and Robin Wakefield, "Success Factors for Deploying Cloud Computing," *Communications of the ACM* 55, no. 9 (September 2012).

acquisition and setup of such a cloud; perceived lack of control for agency directors; increased vulnerability of sensitive data routed through third party vendors, possibly resulting in non-compliance with oversight agencies; resistance among executive managers; and lastly, some state information technology (IT) control agencies will not support a change to their existing enterprise architectures.

Agencies would also need to address a myriad of very important issues not currently seen as potential problems in a traditional communications center model. For example, continuous availability and assured capacity of the cloud, identity management of users, periodic third-party audits, continuous monitoring, encryption of active and stored data residing on the cloud, resistance of political leaders and control agencies, infrastructure limitations, and the certification and accreditation of hosting systems and processes are a few of the concerns that exist. It is possible that some of these concerns have been examined, and solutions to some may exist, however, further research will be required in order to determine the status of their resolution and/or whether they remain as unaddressed issues. With that in mind, the potential to make positive strides in establishing redundant communications centers, partnering with other agencies to share implementation costs, minimizing the carbon footprint created by large communications centers, or freeing up personnel positions by outsourcing IT responsibilities to an outside provider are all potential benefits that should be evaluated.

By contrast, there are a variety of reasons that migration to a Cloud-based system would be supported. First, redundancy options exist, making it viable for emergency/mission-critical communications; agencies will experience additional IT options not found in current enterprise architecture; in the long-run, less money will be spent on maintenance of cloud-based systems; less IT personnel hours would be expended by migrating to a solution hosted by a third party, thereby freeing up additional personnel positions for reallocation; agencies will reduce their carbon footprint; agencies with a certified data center could host a private cloud and allow other mission-critical entities to lease data space; and, as mentioned above, federal government support of migration to the cloud is expanding.

B. RESEARCH QUESTION

Completion of a thesis on how emerging technologies will impact public safety communications centers was intended to further the discussion on whether the public safety community is prepared for the new technologies that will likely become commonplace over the next several years and how to prepare to integrate those technologies into existing structures. The primary research question was designed to answer: "What is the role of cloud-based solutions in public safety communications centers?"

In order to respond to the primary research question, this thesis sought to answer two ancillary questions.

- What are the barriers associated with implementing cloud-based solutions in public safety communications centers?
- How can public safety communications center leaders mitigate those implementation barriers?

C. METHOD

The CIA (CIA) is a variance of the policy analysis method. This thesis will rely on a pre-collected data set concerning the risks, structure, governance, policy and external influences associated with public safety communications centers in light of emerging technological advancements. Because the use of cloud-based and/or managed solutions is a relatively new advancement in the public safety sector, there is limited formal data or literature available. This is further compounded by the varying ideas, perceptions and skepticism associated with unfamiliar and rapidly evolving technologies. In order to narrow the scope of the research, data collected during a nominal group technique (NGT) exercise, which was conducted in 2011 in northern California, will be analyzed. The NGT, further described in Chapter III, utilized the collective experience of a variety of individuals with a variety of roles in the public safety sector, to determine what trends and events are of concern to those actively involved in the leadership of public safety communications centers, development of emerging technologies and implementation of governance models used by the various agencies.

The CIA is an analytical approach to the probabilities of an item in a forecasted set – in this case, the NGT trends and events.[2] Since we know that most events and trends are in some way related to others, a researcher can use their expertise to evaluate the potential interactions among the variables. The ability to understand and document such interactions proves to be valuable in many situations, especially decision making and prioritizing.[3] While often done in groups, "individual experts may estimate the probabilities."[4] The CIA is a quick and effective process that can help to understand the correlation between the two variables, as it is an analytical approach to determine the probabilities in a forecasted set of data.[5]

An initial estimate as to the potential impact of events upon the more prominent trends was conducted. The CIA highlights the panel's assessment of the impacts of each event on each trend. Those probabilities indicate the likelihood of those events occurring within a given timeframe. The panel members were instructed to use the range of -5 to +5, with zero reflecting no impact. The process was repeated for the various trends identified. In the end, several trends and events caused the most significant concerns for the panel members.

This CIA captured a snapshot of what impact each event would have on the trend listed. The background of each evaluator, coupled with the interpretation of the environmental factors present during that time clearly influenced the rankings applied to each relationship. Over time, those influences will likely change, as will the interpretations of varying evaluators.

While it is natural to assume that an identifiable trend will continue its momentum in the same direction and at a consistent rate, one or more events may influence the course of a trend, or stop it in its tracks. Changes to a single trend may affect other trends that were otherwise unaffected by the event affecting the first trend. Therefore, it is

---

[2] Theodore Gordon, "Cross-Impact Method," *AC/UNU Millennium Project*, 1994.

[3] The Vision Center for Futures Creation, "Trend Analysis," accessed January 10, 2014, http:/www.framtidsbygget.se/E/trendanalys/index.htm.

[4] Gordon, "Cross-Impact Method."

[5] Ibid.

important to revisit the initial data and re-calculate the various relationships as a result of technological developments, as well as the current fiscal and political climate. As a component of this thesis, the initial listing of trends and events will be utilized and a new CIA conducted. This will allow the researcher to validate the initial findings and trends. Based on the revised data analysis, a new forecast of important issues may arise, resulting in a new sampling of concerns to be researched, or, the new data may reveal similar priorities to those noted in the initial CIA, which would emphasize the continued relevance of those issues.

The events and trends, which are perceived to have the greatest impact should they merge and occur, will be reviewed and analyzed during the development of the thesis. As described in Bardach's *A Practical Guide for Policy Analysis*, there is an eightfold path to more effective problem solving.[6] Although not each step is required, the eightfold path includes; defining the problem, assembling evidence, constructing alternatives, selecting criteria, projects outcomes, confronting the trade-offs, deciding, and telling the story.

D. THEORETICAL SENSITIVITY

As a law enforcement manager with a strong background in information technology and public safety communications, the researcher has some inherent bias based on professional experience in a large statewide law enforcement agency.

Many large departments, particularly those with multiple communications centers, struggle to adopt emerging technologies in a timely manner, often because of capital outlay cost and because of the challenges associated with training a large number of people over a large geographic region. Even small advancements result in multi-year rollouts and require extensive staff time. Furthermore, the delays caused by internal governmental oversight groups, especially in light of several failed technology implementation projects, may result in frustration or an unwillingness to attempt the evaluation or implementation of an emerging technological advancement.

[6] Eugene Bardach, *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving* (Thousand Oaks, CA: CQ Press, 2012).

Through the completion of this thesis and its accompanying research, a concerted effort was made to remain impartial and open to a variety of concepts and ideas. For example, concepts and opportunities that may prove unrealistic in a large department, but may dramatically improve the effectiveness of a small or medium-sized agency, were evaluated and documented in the most impartial manner possible. Since personal knowledge was a driving force in the research, there are presumably some unknown biases that may have contributed to the overall outcome.

E. LITERATURE REVIEW

The historical descriptions and factual information regarding communications centers can be found in a variety of publications, from trade magazines to introductory segments of issue papers, to government reports and strategy documents. There are also several academic sources that outline some theoretical principles dealing with segments of cloud research. Much of the information is relatively consistent and not usually disputed, as it is often viewed as "known information" throughout the industry.

1. What Is "The Cloud"

In 2011, the National Institute of Standards and Technology (NIST) released Special Publication 800-145, entitled *The NIST Definition of Cloud Computing*.[7] The document lists five essential characteristics that comprise the cloud model: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. It also lists four common deployment models: the private cloud, community cloud, public cloud and hybrid cloud. The information contained in this document is consistent with the introductory segments of dozens of additional publications, varying from governmental reports to trade magazine articles to academic writings. Therefore, for the purposes of this report, the definition of the various types of clouds and their characteristics are not disputed.

[7] U.S. Department of Commerce, National Institute of Science and Technology, *The NIST Definition of Cloud Computing*, September 2011.

2. What We Know

The literature specific to cloud-based, first responder communications centers is virtually non-existent, especially in governmental and academic publications. However, the information relative to cloud-based operating systems is expanding rapidly and can be divided into several categories: studies commissioned by an agency, or group of agencies, to explore the concept of cloud computing and its applicability to use in governmental organizations; trade magazine articles, academic publications exploring the theoretical adoption of technology systems, and a variety of industry-based publications focusing on the security aspects and concerns associated with cloud computing.

a. Studies and Reports by Government

In December 2010, the U.S. Chief Information Officer released the *25-Point Implementation Plan to Reform Federal IT Management* in order to improve the technological efficiency of the federal government.[8] Perhaps the most significant and daunting of the recommendations was to shift federal agencies to a "cloud first" policy. Since the release of that plan, a number of "studies" have been completed to examine and make recommendations regarding the implementation of cloud-based initiatives within the government. Most of the studies are generated by federal agencies, as that is where the initial direction originated. Some of the studies are a top-to-bottom overview of the key factors, such as the Congressional Research Service's *Overview and Issues for Implementation of the Federal Cloud Computing Initiative*.[9] Other studies examined for this review contained similar outline structures as those listed below.[10]

- Considerations for adoption of cloud computing (cost, energy efficiency, availability, scalability, security, reliability)
- Alignment with the *25-Point Implementation Plan to Reform Federal IT Management*

[8] White House, *25 Point Implementation Plan to Reform Federal Information Technology* (Washington, DC: White House, December 9, 2010).

[9] Eric A. Fischer and Patricia Moloney Figliola, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*, CRS Report R42887 (Washington, DC: Library of Congress, Congressional Research Service, January 4, 2013).

[10] Additional studies are included in the reference list.

- Internal drivers to adoption of the cloud (budget, consolidation)
- Internal challenges to adoption of the cloud (security, IT knowledge, interoperability)

In addition to the overview documents, there are strategy documents, specifically from the Department of Homeland Security and the Department of Defense. The documents make reference to several of the issues noted above, including a strong emphasis on cyber security. The respective agency directors also establish a road map for how the cloud will be integrated into their agencies. These publications are timely, with updated documents released frequently. This underlines the relative recency and rapid evolution of this topic/field.

b. Studies by Foreign Governmental Entities

Two publications drafted by the European Network and Information Security Agency are quite relevant to the decision-making process regarding cloud migration: *Security and Resilience in Governmental Clouds* and *Cloud Computing, Benefits, Risks and Recommendations for Information Security* provide substantial risk analysis models and tools.[11] The first dedicates an entire chapter to SWOT analysis of public and community clouds, while the second provides an in-depth analysis of policy, technical, legal, and other risks. This information provides a foundation for agencies who are contemplating a cloud-based strategy.

c. Trade

Trade magazines are on the whole, neutral toward the topics they are addressing, and tend simply to report on a recent feasibility study or a governmental decision to move ahead with proposed idea or practice or discuss the advantages and disadvantages of a

[11] European Network and Information Security Agency, *Cloud Computing; Benefits, Risks, and Recommendations for Information Security*, Crete, Greece, 2009; European Network and Information Security Agency, *Security and Resilience in Governmental Clouds*, Crete, Greece, 2011; European Network and Information Security Agency, *Cloud Computing; Benefits, Risks, and Recommendations for Information Security*.

practice.[12] Only one appears to exist specific to law enforcement or public safety operations.

The sole article published in a law enforcement magazine also addresses the ability of the cloud to lower costs and is geared towards the challenges being faced by most departments in light of diminishing resources and dwindling budgets. The article, written by marketing officer for a worldwide IT provider, is one of few that specifies a potential cost savings for agencies who migrate to a hosted Software as a Solution service.[13] The product may be valuable and viable option; however, in light of the author's potential bias as a salesperson for the service, additional impartial research should be conducted.

d. Academic

In addition to several academic articles that deal with security concerns in the cloud (detailed in the next section), there are some articles that discuss theories and even a mathematical problem-solving model of data storage in the cloud. The mathematical model contained in "A Model and Decision Procedure for Data Storage in Cloud Computing" has limited application to public safety communications centers functioning in the Cloud, because it describes a model that takes "output lists of compatible storage services and constructs an integer linear programming problem."[14] Essentially, it uses performance characteristics, such as bandwidth, job turnaround time and latency and shows that by using cloud-based applications, complex problems can be solved more quickly, often within one second. The importance of such functionality becomes evident when compared to a similarly complex environment, such as a dispatch center, where a multitude of critical functions must be processed simultaneously.

The "technology adoption life cycle," "innovation decision process theory," and "perceived attributes theory" are all discussed in "Cloud Computing: From Hype to

---

[12] Ryan Coutinho, "Cloud Computing or Cloudy Computing," *Public Management*, April 2012, 23.

[13] Ian Archbell, "Use the Cloud to Lower Sky-High Costs," *Law Enforcement Technology Magazine*, March 2011, 54.

[14] Arkaitz Ruiz-Alvarez and Marty Humphrey, "A Model and Decision Procedure for Data Storage in Cloud Computing," *IEEE Computer Society*, 2012, 572.

Reality."[15] The probable evolution of cloud computing and rate of adoption is helpful in determining how prolific cloud-based infrastructures will become. As a relatively new technology, it is important to recognize the five stages an adopter will go through acquiring knowledge, persuasion, decision, implementation and confirmation. Understanding how the new technology will be judged can assist the developer in achieving success. The characteristics include trial ability, operability, relative advantage, complexity and compatibility.[16]

3. Security Concerns

The most significant amount of literature germane to this project is specific to security concerns associated with cloud-based infrastructure. A variety of publications, particularly from within the industry, outline the security concerns, considerations, vulnerabilities, challenges and approaches to cloud security.

Law enforcement agency directors must ensure the clouds they utilize will maintain the integrity of the data stored there. In 2002, the federal government established the Federal Information Security Management Act (FISMA), which established strict information security protocols, but prior to the advent of the cloud.[17] Nevertheless, many public safety agency directors felt physical control of their data was a necessity, meaning data servers must be at a secure location, such as their police station. The public sector, meanwhile, has embraced the need for secure cloud space and created specific segments that meet the FISMA standards, such as Google Apps for Government, which provides segregated systems for U.S. government customers and for which the data are stored exclusively in the United States.[18]

---

[15] Ramkumar Dargha, "Cloud Computing: From Hype to Reality. Fast Tracking Cloud Adoption," presented at the International Conference on Advances in Computing, Communications and Informatics, Chennai, T Nadu, India, August 3–5, 2012, 440.

[16] Dargha, "Cloud Computing: From Hype to Reality. Fast Tracking Cloud Adoption," 440.

[17] *Federal Information Security Management Act of 2002*, Washington, DC, 2002.

[18] "Security," accessed January 18, 2013, http://www.google.com/enterprise/apps/government/benefits.html?section=security.

In 2011, Federal Chief Information Officer Steven VanRoekel said that the White House's Office of Management and Budget would launch the Federal Risk and Authorization Management Program (FedRAMP), a unified government-wide risk management initiative focused on providing security for cloud-based systems.[19] The program offers a standard approach to conduct security assessments of cloud systems based on an accepted set of baseline controls and consistent processes vetted and agreed upon by agencies across the federal government. To date, each federal agency has gone through multiple steps that take anywhere from six to 18 months and countless man hours to properly assess and authorize the security of a system before it grants authority to transition to the cloud.[20]

In what is perhaps the strongest indicator of confidence in the security of the Cloud, in December 2010 the Office of Management and Budget declared that the federal government now operates under a "cloud-first" policy. This means that agencies must first try to incorporate some type of cloud computing into each IT project under consideration.[21] Nicholas Popp, Vice President of Product Management and Development at Symantec, acknowledged in an interview that the cloud is not quite up to par with on-premise installations when it comes to security. He predicted that between 2015 and 2017, the cloud would be the more secure environment for small and mid-sized businesses.[22]

Although there is documentation showing federal government support of movement to Cloud-based platforms, there are certainly concerns regarding information

---

[19] U.S. General Services Administration, "About FedRAMP," last reviewed March 25, 2014, http://www.gsa.gov/portal/category/102375.

[20] John Higgins, "Feds Aim to Lock Down the Cloud," *Technology News World*, December 13, 2011, http://www.technewsworld.com/story/73956.html.

[21] Federal Computer Week, "When the Cloud Makes Sense," 2011, http://fcw.com/Downloading CloudComputing.

[22] Thor Olavsrud, Security in the Cloud Is All About Visibility and Control. *Network World*, February 17, 2012. http://www.networkworld.com/research/2012/021812-security-in-the-cloud-is-256332.html?page=3.

stored there. The Open Web Application Security Project published a list of the top 10 cloud security risks and at the top of the list is "accountability and data ownership."[23]

4. Studying the Future

The ability to effective deal with problems and issues depends on how well prepared you are. For many people, until problems present themselves in a current, relevant situation, little thought is given toward advance preparation. Several universities have developed educational programs aimed at better preparing people for what the future might bring, including the University of Houston, which offers a Master of Science degree in foresight. Professional futurists emphasize systemic and transformational change and they describe alternative plausible and preferable futures, in addition to the expected future. Futurists also use a balance of qualitative and quantitative tools. By understanding the variables and addressing potential outcomes, it is possible to gain a clearer perspective of what challenges lie ahead. Futures study, futuring and futurism are a few of the terms given to the body of techniques and knowledge given to the process of modeling the future through the use of strategic foresight.[24]

In their book, *Thinking About the Future, Guidelines for Strategic Foresight*, Dr. Andy Hines and Dr. Peter Bishop describe the framework associated with strategic foresight. There are six steps (summarized below) that have been described by the Association of Professional Futurists' professional development team as "fundamental" to creating a comprehensive strategic foresight.[25]

- Framing—guidelines regarding attitude, audience, work environment, rationale and purpose, objectives, and teams.
- Scanning—the system, history, and context of the issue and how to scan for information regarding the future of the issue.

---

[23] OWASP, "Cloud Top 10 Security Risks," last modified January 23, 2014, https://www.owasp.org/index.php/Category:OWASP_Cloud_-_10_Project.

[24] Edward Cornish, *Futuring—The Exploration of the Future. World Future Society* (Bethesda, MD: World Future Society, 2004), ISBN 0-930242-61-0.

[25] Peter Bishop and Andy Hines, *Thinking About the Future, Guidelines for Strategic Foresight* (Washington, DC: Social Technologies, LLC, 2006), ISBN-13: 978-0-9789317-0-4.

- Forecasting—by using the information derived in the scanning process, one can prepare guidelines regarding drivers and uncertainties, tools, diverging and converging approaches, and alternatives.
- Visioning—guidelines focused on thinking through the implications of the forecast and envisioning designed outcomes for the organization.
- Planning—guidelines that develop the strategy and options for carrying out the Vision.
- Acting—guidelines for communicating the results, developing action agendas, and institutionalizing strategic thinking and intelligence systems.

Many Fortune 500 companies use future modeling to determine the long-range strategy that will allow their company to stay one step ahead of the competition, while still understanding how the market will evolve. Those that have succeeded are some of the most profitable companies in existence, such as Kellogg's and General Mills. Others who have failed to anticipate the changes in the market have suffered tremendous losses, such as Eastman Kodak.

F. DEFINITION OF TERMS

1. Communications Center

Communications (or dispatch) centers come in a wide array of shapes and sizes. Some departments have one dispatch center; others may have multiple centers, depending on the size of the agency and their geographic responsibility. Communications centers may house multiple agencies and even various public safety disciplines (law enforcement, fire, and emergency medical services). Dispatch centers in small communities may only have one or two operators at a time, however, in a large metropolitan area; a center may have up to 100 people working at any given time. The role of the dispatcher involves answering routine and emergency telephone calls from the public, reacting to requests for assistance from other public safety entities, documenting incidents via a computerized system, dispatching personnel using voice or data systems, and tracking/logging the disposition of calls for service.

Dispatch centers that receive 9-1-1 emergency calls are often referred to as a public safety answering point (PSAP). It is estimated that there are now over 7,500 PSAP

in the United States.[26] The vast majority of PSAP are relatively small and associated with a single municipal or county public safety agency. For example, in California, 56% of the state's PSAP have only three workstations or fewer.[27] However, some are consolidated 9-1-1 emergency dispatch centers servicing multiple agencies.

In order to maintain the newest technologies, considerable investments in infrastructure are necessary. The initial outlay costs are often prohibitive and, in order to remain on the cutting edge, the need to frequently invest substantial capital poses a tremendous challenge for many agencies, especially smaller departments. Equipment may include a computer-aided dispatch (CAD) system, which allows an operator to enter the type of call, location, pertinent details regarding the incident and the name of the reporting party. That call may be electronically transmitted to a police or fire vehicle via computer and the responding unit can then see all of the relevant information. Additionally, the dispatcher may utilize a radio system to transmit the details over the airwaves.

2. The 9-1-1 System

The first 9-1-1 system was installed as a way to quickly connect a subscriber to the local police station. This system did not automatically identify the caller but did provide a means to access emergency services that had not previously been available. The rudimentary 9-1-1 system evolved quickly and was improved by other telephone companies to become the enhanced 9-1-1 (E9-1-1) system, which provides both caller location and identification. E9-1-1 is currently deployed in most metropolitan areas in the United States and Canada. A more recent phase of E9-1-1 service allows a cellular telephone to be located geographically using some form of location data from the cellular network, or by using, a global positioning system (GPS) built into the phone itself.

Trends in telecommunications mobility and technology convergence, and the growing market penetration of both cellular and VoIP telephony have underscored the

[26] Federal Communications Commission, "PSAP Registry," January 4, 2013, http://transition.fcc.gov/pshs/services/911-services/enhanced911/psapregistry.html.

[27] California Office of the Chief Information Officer, "California 9-1-1 Strategic Plan," July 30, 2010, http://www.cta.ca.gov/PSCO/911/pdf/911_Strategic_Plan.pdf.

limitations of the current 9-1-1 infrastructure. The nation's 9-1-1 system, now based on decades-old technology, cannot handle the applications that are increasingly common in personal communications and critical to future public safety advances.

Although the 9-1-1 system has served us well for many years, the current architecture is becoming outdated as new technologies become commonplace. New forms of communication, such as text messaging, are not supported by the current 9-1-1 system. Due to these changes in technologies, the USDOT and NENA began looking at technologies to provide the platform for the NG9-1-1.

Figure 1 outlines the way a 9-1-1 call is handled in today's E9-1-1 environment. Starting from the landline caller on the left side of the diagram, the 911 call is received at the phone company's central office (CO). From there, it is identified as a 911 call and is transferred to the selective router. The selective router uses software tables to determine the appropriate PSAP, based upon the location of the caller. From the selective router, the call is transferred directly to the PSAP via 911 'trunks.' These 911 lines are hardwire telephone circuits. They are referred to as CAMA (centralized automatic message accounting), which carries the calling party information "inband" or with the call on the circuit. They are sometimes SS7 (Signaling System 7), which uses a separate data circuit for call information and switching.

Once at the PSAP, the telephone switch receives the 911 call and sends a request to the automatic location identification (ALI) database to receive the specific address associated with that phone number. At this point, the 911 call, along with the location information is provided to the Call Taker. Although it seems like a lengthy process, it takes only milliseconds to reach the Call Taker.

Wireless 911 calls are sent to the selective router from the wireless carrier, along with some basic location information for the purpose of routing the call to the appropriate PSAP. At the same time the call is being sent to the selective router, the wireless carrier sends more detailed location information (based upon triangulation or GPS depending upon the wireless carrier) to the ALI database. From there, the call follows the same route as the landline call.

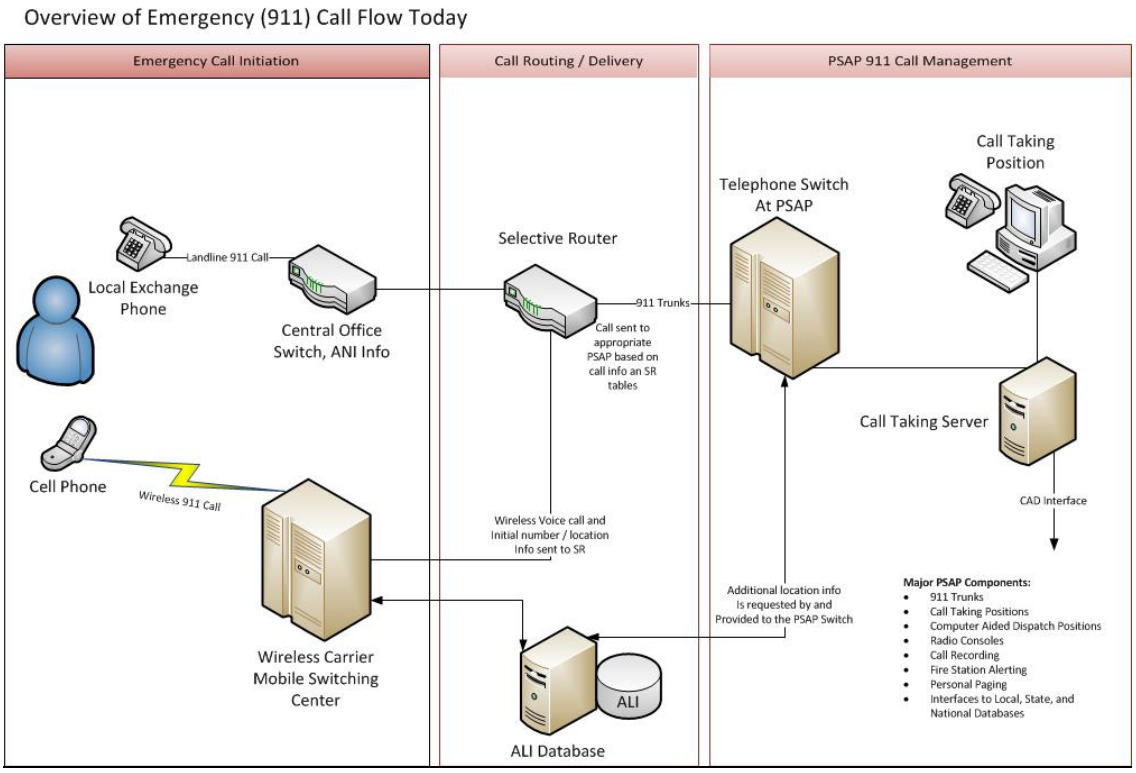

Figure 1. Overview of Emergency (9-1-1) Call Flow Today

3. Next Generation 9–1-1

NG9-1-1 is envisioned as a new internetwork that will provide the foundation for public emergency services in an increasingly mobile and technologically diverse society. Ultimately, the goal of NG9-1-1 is to enable E9-1-1 calls from most types of communication devices and provide:

- Quicker and more accurate information public safety first responders
- Better and more useful forms of information (data, images, and video)
- More flexible, secure and robust PSAP operations
- Lower initial capital outlay and reduced operating costs for public safety communications centers

Internet protocol (IP) is a protocol, which defines how data is sent from one computer or device to another, on data networks, such as the Internet. Each device has a unique identifier, or address (also known as the IP address). Data is transmitted in packets, which are small chunks of the message being delivered from one IP address to another.

By utilizing IP technology, NG9-1-1 will move the transport and management of a traditional 9-1-1 call from switched voice circuits and multiple discreet components to an integrated data and voice transport mechanism.

Although NG9-1-1 uses the same protocol as the Internet, an NG9-1-1 network needs to be secure from outside intrusion and any unauthorized access to data. Levels of security for portions of the information are dictated by the Department of Justice (DOJ) and will be required to meet security standards as defined for an emergency 9-1-1 call.

NG9-1-1 will change the core capabilities of emergency services in three areas:

- Types of calls received
- Ability to transfer/receive calls from PSAPs outside the local region
- Capability to accept additional information designed to facilitate emergency services

These are expansions of current functions, not fundamentally new roles.

NG9-1-1 is in varying stages of development and deployment throughout the United States. The basis for NG9-1-1 is the use of IP, which allows for the acceptance of sources other than simply voice calls. Also, an NG9-1-1 network allows for much more flexibility in the routing and transferring of calls and data.

Some of the potential benefits of NG9-1-1 include:

- Ability to accept multimedia calls for help, including:
    - voice
    - video
    - text
    - instant messaging
    - pictures
    - highway/security cameras
    - alarms
    - sensors
    - personal medical devices
    - telematics (on-star type devices)
    -

- ability to route overflow calls to other PSAPs
- improved routing of calls, based upon location and status of the PSAP
- ability to isolate calls from a specific incident (based upon location) and queue those calls separately from all incoming 911 calls
- ability to transfer calls from one PSAP to another along with the associated location data, call-taker notes, text/video/pictures, etc.
- enhanced reporting capabilities

Because NG9-1-1 uses an IP platform, the potential is for different products and networks to interconnect and share data in accordance with the rules developed by the participating agencies. NENA is working on the development of standards for NG9-1-1 to enhance this potential.

In an initial NG9-1-1 environment, there may be some slight variation to the flow described in Figure 2, but in all cases, the landline 911 call will still go to the phone company's central office first. From there, the call will be transferred into an IP-based NG9-1-1 network. The interface between the phone company's central office and the NG9-1-1 network varies by vendor, as in some cases the phone company is providing the central office services and the NG9-1-1 network, and in others, the NG9-1-1 network is owned and operated by a third party.

Once in the NG9-1-1 network, the call is routed to the appropriate PSAP based upon multiple factors, including the location of the caller and the status of the PSAPs. In an NG9-1-1 environment, the existing selective routers will no longer be used. Until all of the agencies in a given state are operating on an NG9-1-1 network, however, the selective routers must remain in place and be interfaced to the NG9-1-1 network.

The call routing and delivery component of NG9-1-1 includes the NG9-1-1 network. This network is sometimes referred to as the cloud, or the emergency services Internet protocol network (ESI Net). These networks are broadband, and can carry large amounts of data. In an NG9-1-1 environment, this is where the call routing, the data transfers, the ALI identification occurs. This NG9-1-1 network can cover one region and connect to other NG9-1-1 networks in neighboring regions. This NG9-1-1 network can also be used to transfer data between the PSAPs and to the mobile computers in the field.

(It is important to note that the mobile computers will still require some form of Internet connectivity to connect to the NG9-1-1 network—in other words, this does not replace the radio or cellular requirement of mobile data).

One of the primary differences between the NG9-1-1 network and the existing analog call routing/delivery is the ability to transfer voice and data within the NG9-1-1 network, as opposed to just voice in the existing analog environment. This is what will allow the PSAPs to receive text messages, photos, video, etc., in a full NG9-1-1 system. The routing can be pre-determined, via policy based upon the following factors:

- location
- call type
- PSAP status
- network status

As mentioned above, once the NG9-1-1 network is in use throughout the state, the existing selective routers are no longer needed. The call routing will occur using a new Automatic Number Identification (ANI)/Automatic Location Identification (ALI) database and intelligent PSAP routing within the network.

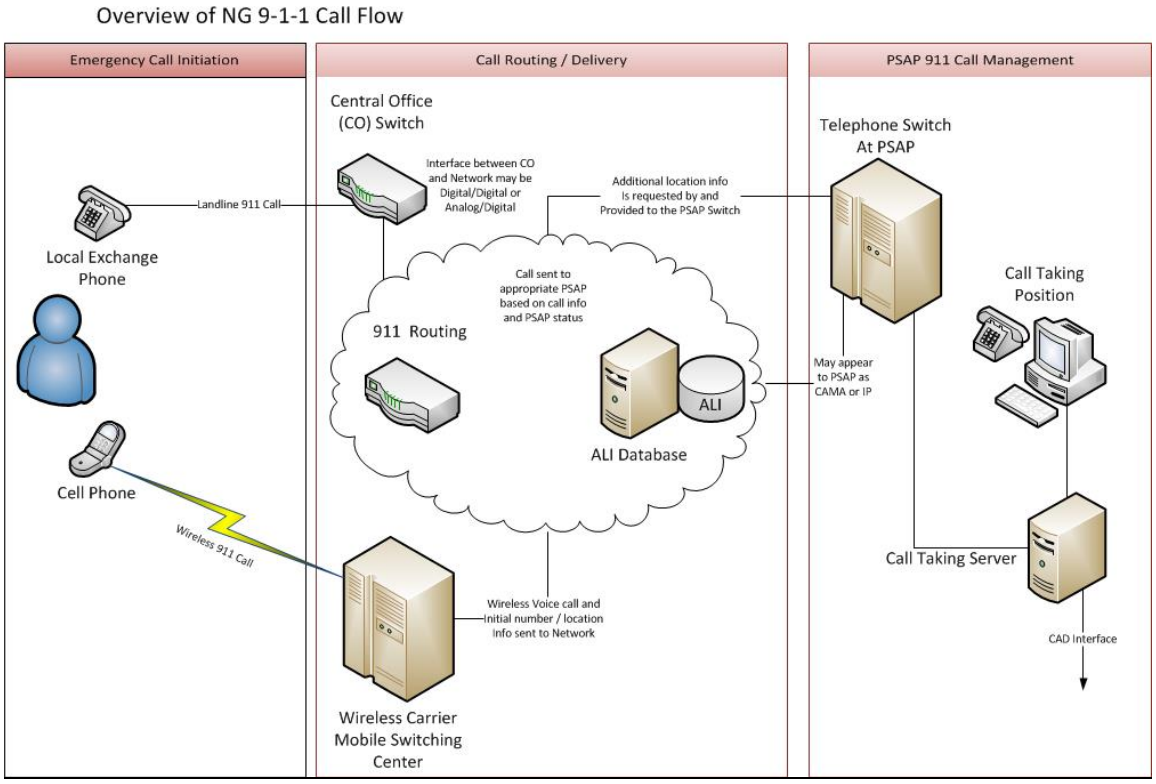

Figure 2. Overview of Next Generation 9-1-1 Call Flow

4. Cloud-Based Computing

"Cloud computing" is essentially Internet-based computing, where shared resources, software and information are provided to computers and other devices on-demand. Although less-refined forms of cloud-based computing, such as IBM's "on-demand" computing have existed since 2003, the actual "cloud" came to fruition in 2006 when Amazon and Microsoft afforded companies the opportunity to store data on their underutilized data servers. The mainstream launch of "Google docs" in January 2010 and Apple's "iCloud" in June 2011, though, caused the popularity of the cloud to explode. With more and more people coming in contact with some form of cloud computing, user acceptance is on the rise. While delivering a keynote speech on February 14, 2012, Apple CEO Tim Cook said there were over 100 million people using its iCloud service.[28]

[28] Matthew Panzarion, "Apple's Tim Cook Says There Are Now Over 100M iCloud Users, Marking 15M User Growth in 21 Days," February 14, 2012, http://thenextweb.com/apple/2012/02/14/apples-tim-cook-announces-that-there-are-now-over-100m-icloud-users-marking-15m-user-growth-in-21-days.

In its simplest form, cloud computing is "shared services."[29] End users are able to access applications, services and files from a variety of remote platforms (e.g., the cloud), including desktop and laptop computers, tablets, smartphones and other small form devices. Concepts like infrastructure as a service (IAAS) and platforms as a service (PAAS) allow agencies to move the information technology responsibilities outside of the department to companies that specialize in that line of work. This affords them the ability to focus on their core mission—public safety—rather than on upgrading virus-prone software and procuring the latest hardware. Memory-intensive software that was once loaded onto individual machines has become a thing of the past; the need for large server rooms requiring constant attention decreases each day. For example, if an agency wants to launch a new records management system, it has the option to work with a vendor who will design a web-based interface to meet its needs. Agency personnel would then enter the data from any computer with access to the Internet and all information would be stored on an off-site server managed by the vendor.

The vendor is ultimately responsible for security and maintenance of the data, ensuring the servers are constantly updated with the latest virus protection and software updates, and making any design modifications or output changes requested by the agency. If the agency selects a records management system that already exists, it can quickly implement it by utilizing the cloud infrastructure without having to acquire significant hardware. This substantially lowers both time and cost barriers to deployment.[30] Ultimately, cloud computing offers the government an opportunity to be more efficient, agile, and innovative through more effective use of IT investments.

In a cloud-based environment, the information technology expertise shifts from on-site to off-site, as technicians housed at the host facility essentially control the system. These facilities may be a few miles away, or thousands of miles away. They are linked through high capacity, lightning-fast connections that allow data to move throughout the world in a matter of milliseconds. Agencies are no longer bound by the capabilities of

[29] *Wikipedia*, s.v., "Cloud Computing," last modified November 17, 2012, http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=523482934.

[30] Vivek Kundra, *25 Point Implementation Plan to Reform Federal IT Management* (Washington, DC: U.S. Government Printing Office, December 2010).

their on-site personnel, who often only have a rudimentary understanding of the system. Full time technicians who specialize in the maintenance of systems are available 24/7/365 through managed systems. They are able to conduct maintenance from their off-site location, install software updates, security patches, etc. When that occurs, they have a built in system of redundancy that allows the user to remain fully active via a separate path.

G. REVIEW OF UPCOMING CHAPTERS

Chapter I provided a framework of the problem faced by public safety leaders as new technologies begin to merge with legacy systems that have been in place for many years. This chapter also discussed the literature reviewed for this thesis and the impact the literature has on the subject matter. Although the introduction of cloud-based technologies to the public safety communications center realm has only been prevalent over the past five years, there is some significant literature describing its implementation and the development of polices and procedures for its use in a variety of applications. Chapter I provided a glimpse into the research methods that will be used to systematically analyze some of the data that is already available. Finally, Chapter I provided an enhanced understanding of terms and concepts associated with public safety communications centers, as well as a discussion regarding the processes currently in place today.

Chapter II describes the data collection process and analysis components. Specifically, the chapter includes the rationale of the nominal group technique and CIA, as well as detailed descriptions of the trends and events that were generated, evaluated and graphed. Chapter III expands on the analysis of various relationships of trends by using current values and comparing them to earlier data sets. Chapter IV provides findings; details implementation concerns and discusses strategic planning methods. This thesis concludes with Chapter V and provides recommendations for moving forward, generalizes the findings and discusses opportunities for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DATA COLLECTION AND ANALYSIS

The ability to deal effectively with problems and issues depends on how well prepared you are. For many people, until the problems present themselves in a current, relevant situation, little thought is given to advance preparation. Professional futurists emphasize systemic and transformational change, as opposed to traditional forecasters and planners who focus on incremental change based on existing conditions and trends. Since long-term predictive forecasts are rarely correct, futurists describe alternative plausible and preferable futures, in addition to the expected future. Instead of limiting themselves to traditional forecasters' quantitative methods, futurists also use a balance of qualitative and quantitative tools.

In 2011, as a component of a leadership development program, this researcher was exposed to several valuable concepts and techniques associated with future studies. Some of those techniques, as well as some of the data collected, provide a valuable foundation for researching how prepared public safety communications centers are for emerging technologies.

A. NOMINAL GROUP TECHNIQUE

The NGT is a structured method of bringing people with different backgrounds and experience together to solicit ideas and opinions regarding a particular issue. In April 2011, a panel of seven professionals, with varying backgrounds in the public safety and information technology fields, met in Sacramento, California, for the purpose for examining and evaluating the role of integrating cloud-based solutions into public safety communications centers.

The NGT process is a face-to-face group process technique that is used to gain consensus. It elicits "opinions and aggregates judgments to increase rationality and creativity when faced with an unstructured problem situation."[31] By using their own experiences, skills and feelings, each participant is able to participate equally in

[31] Peter Delp at al., *System Tools for Project Planning* (Bloomington, IN: International Development Institute, 1977).

evaluating or identifying issues before nominating his or her priority issues, and then ranking them on a pre-determined scale. During this initial stage, no discussion is allowed between the participants, encouraging the free expression of all ideas. The process allows for all group members to list as many responses as possible.

During the course of the NGT exercise, the panel members were asked to examine two different dimensions regarding the potential applications for the issue. Those dimensions were the issues associated with future trends and events. Once all participants prepared their list, the NGT leader (a non-participant) documented all ideas on a flip chart where everyone else could see the ideas generated. After collectively identifying the trends and events, and quantify the ideas and opinions of the panelists, the results identified any disparities within the group on each of the evaluated trends and events. Eventually, each item was briefly discussed among the participants. Ultimately, that generated some thoughtful and interesting discussions, as various members of the group attempt to persuade others to think differently about their particular assessments. They indicated their preference by weighing items against the others. During the 2011 NGT, the acceptable range was 1–200. The outcome is the mathematical aggregation of each participant's preferences.[32] This process ensures that all members of the group are able to make an equal contribution regardless of how effectively (or ineffectively) they contribute to the dialogue.

B. TRENDS

A trend is a series of incidents or events taking place, which seems to indicate a direction in which a particular issue may be heading. It is based on past, present and future, and can be quantitative or qualitative. A trend usually has a social, technological, economic, environmental or political characteristic. The panelists were asked to name trends they felt were occurring that would have an impact, positive or negative, on the role of integrating cloud-based solutions into public safety communications centers.

Once the trends were selected, all panelists individually rated them on different criteria. The first criteria included the "level of impact" the trend had on the issue five

[32] Delp et al., *System Tools for Project Planning*.

years in the past, the projected "level of impact" the trend would have on the issue five years in the future and ten years in the future. A baseline number of 100 was utilized to denote the current level of impact.

Table 1 provides a sample of the level of impact and level of concern. Trend #1 is viewed as increasing in five years to 150 and doubling from its current baseline of 100 in 10 years to 200. Additionally, Trend #1 is perceived to be fifty, or only half the value, when comparing it five years in the past (-5) to the established baseline today. Thus, the first trend in the example table is viewed as constantly increasing over a twenty-year period. The second trend, Trend #2, was twice as high (200) five years ago when comparing it to the baseline of today (100). This second trend decreases in veracity to seventy-five and then to twenty-five and ten years in the future, respectively. Trend #2 is observed to be constantly decreasing over time.

Table 1. Sample Trends—Level of Impact and Concern

Trend	-5 Yrs (Past)	Today (Baseline)	+5 Yrs (Future)	+10 Yrs (Future)	Concern (1–10)
Trend #1	50	100	150	200	**9**
Trend #2	200	100	75	25	**5**

Finally, the panelists were asked to provide an individual level of concern for each trend as it related to the issue. Utilizing numbers between one and ten (one for a low level of concerns and 10 for a high level of concern) the panel measured the perceived level of impact of the trend on the issue being discussed. A higher number posted in the concern column indicated the panelist's opinion that the trend would have great impact. The example table depicts a high level of concern with a measurement of nine.

- 2011 NGT Results—Trends

Initially, the group identified 26 potential trends. Each panelist was given the opportunity to select the ten trends they felt were most relevant to the issue. Once all of those ratings were completed, they were collected and entered into a spreadsheet. The

average and median numbers were determined and the median numbers were charted in the trend summary table (Table 2).

Table 2. Trend Summary Table

Identified Trends	-5 Yrs (Past)	Today (Baseline)	+5 Yrs (Future)	+10 Yrs (Future)	Concern (1–10)
T1 = State of Economy—Fiscal	100	100	125	150	**8**
T2 = Consolidation and Regionalization of Resources	50	100	150	150	**8**
T3 = Standardization of Technologies	50	100	150	160	**8**
T4 = Reliability of the Cloud	25	100	175	200	**10**
T5 = Mobility	50	100	160	200	**8**
T6 = Outsourcing	20	100	140	150	**8**
T7 = Security with the Cloud	30	100	150	200	**10**
T8 = Political Ramifications	75	100	125	150	**9**
T9 = Availability of Shared Resources—Infrastructure	50	100	150	200	**7**
T10 = Personnel Oversight	100	100	150	150	**6**

Trend 1 = State of the Economy—Fiscal

The panel agreed that one of the key driving forces would most likely always include the state of the economy. A lack of funding creates hurdles, but at the same time, may create unforeseen opportunities. By being forced to look at the situation from a new perspective, agencies may be forced to investigate technologies that they previously disregarded.

Trend 2 = Consolidation and Regionalization of Resources

As budgets shrink and staff are eliminated, the consolidation and/or regionalization models begin to look brighter and brighter. Infrastructure costs are steep and maintaining data centers, multiple communications centers, buildings, etc may not be

feasible. Therefore, agencies may reduce the number of facilities they maintain and the smaller agencies may explore partnerships with like organizations in order to achieve costs savings.

Trend 3 = Standardization of Technologies

As new technologies develop, the standardization of systems will be an important component of their success. “One-off” systems and customized systems have become increasingly difficult and expensive to support. Many organizations do not have the ability to keep technical support people on staff; therefore, commercial off-the-shelf (COTS) systems are becoming more popular. It will be important for vendors to use open-source technology in order to allow their software to work with a variety of other platforms.

Trend 4 = Reliability of the Cloud

The reliability of the cloud was seen as one of the most concerning issues among the panel members. Recognizing that our systems will likely evolve into cloud-based platforms over the next five to ten years, the reliability of the cloud infrastructure is critical. Over the past several years, acceptance of the cloud has increased, but there is still extensive work to be done.

Trend 5 = Mobility

The panel agreed that the ability to move operations from one place to another is very attractive, especially if it can be done quickly and seamlessly. Not only would this be beneficial during emergency incidents or large-scale events, but it may be applicable when trying to maintain reasonable call volumes, or when attempting to circumvent a system outage affecting the local carrier. Additionally, in smaller operations, it may afford an agency the ability to move their operations off-site or to another small entity in order to share personnel resources.

Trend 6 = Outsourcing

The panel discussed several types of outsourcing. They included the outsourcing of system development and maintenance, as well as the outsourcing of dispatch services

from within the agency. In the end, the discussion focused on the outsourcing of system development and maintenance and the ability of an agency to get prompt and personalized service when they needed it. As an example, if the CAD system needed new "type codes" added, would that require someone from the vendor to respond, or could it be accomplished "on-the-fly" by a local employee. On a more complex note, could call traffic be re-directed on a Sunday afternoon if necessary, or would it have to wait until Monday for the vendor to arrive on site.

Trend 7 = Security with the Cloud

Similar to the reliability of the cloud, the security of the data residing in cyberspace is a critically important trend. With limited cloud users five years ago, the level of impact was minimal, but as more and more users migrate to cloud-based systems, security concerns and threats will increase rapidly. Employing a system that does not reside within the private data center of an organization or agency is an uncomfortable prospect for many executives and IT professionals.

Trend 8 = Political Ramifications

The reality is that our ability to change and the flexibility in our decision making process is often driven by politics. It may be related to selection of a specific vendor or product or merely the appearance that a certain decision may cast. Additionally, the movement or placement of communications centers also has political ramifications. Cities and counties often lobby to have a local dispatch center in hopes that they will receive more personalized service. Ultimately, the decision on where to house a dispatch center or whether or not to eliminate one may not rest with the agency director.

Trend 9 = Availability of Shared Resources

Sharing resources often results in less control over the resource, but it likely means that more resources are available and oftentimes at a lesser cost. The panel discussed that there would likely be a positive benefit in sharing the infrastructure cost burden among multiple users. They also discussed the fact there would likely be a "menu" of options from which to choose and it would give the agency greater flexibility in picking and choosing between various options.

Trend 10 = Personnel Oversight

The ability to manage personnel is a challenge in the best of environments. This trend was explored because a discussion occurred regarding the negative impact that may be felt if employees were assigned to work in remote locations or from places where supervision is minimal or non-existent. Questions that surfaced included; would their performance suffer? Would their allegiance or connection to the agency be diminished?

Table 3 synthesizes the average numerical value assessed by the panelists. It is important to note that in 2011, the NGT panel projected the trends that would show an upward rise in 2016 would likely include reliability of the cloud (175), mobility (166), and security of the cloud (161). As several years have passed, the accuracy of the NGT panelists' estimation appears clearer, with those trends becoming more prevalent in today's public safety communications center environment. Figure 3 depicts those numerical values in a graphical manner.

Table 3. Trends Analysis Table—Level of Impact

Average ~ -5/+5/+10 Years					
	-5 Years	**Today**	**+5 Years**	**+10 Years**	**Concern 1–10**
State of Economy	91	100	135	154	
Consolidation	56	100	133	134	
Standardization of Tech	65	100	146	159	
Reliability of Cloud	22	100	175	186	
Mobility	61	100	166	186	
Outsourcing	40	100	131	153	
Security of Cloud	44	100	161	179	
Political Ramifications	68	100	125	150	
Avail of Shared Resources	58	100	153	181	
Personnel Oversight	62	100	114	130	

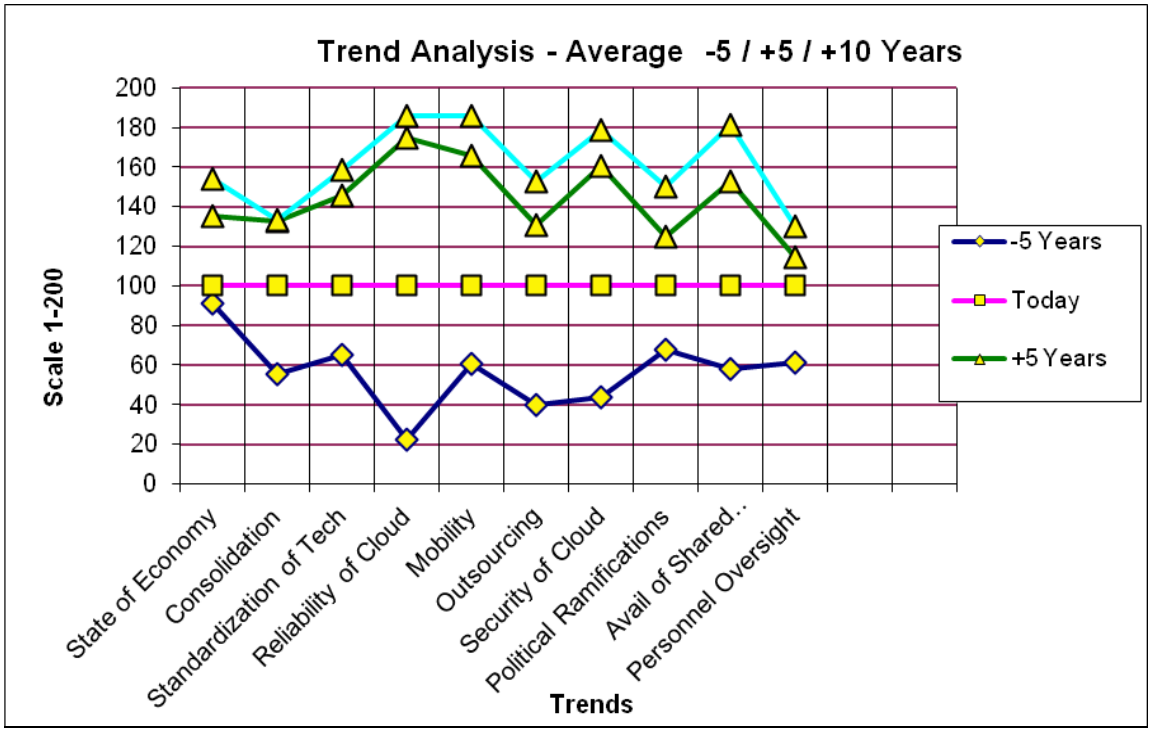

Figure 3. Trend Analysis Graph—Level of Impact

Similar to the 2011 NGT trend projection, Table 4 shows the level of concern for each trend. The two trends that received the highest level of concern were the reliability of the cloud (10) and the security of the cloud (10). As proliferation of cloud-based architecture increases, two of the most discussed concerns revolve around the reliability and security of cloud-based systems. Again, it appears that the concerns identified by the panelists in 2011 are coming into focus today. Figure 4 depicts those numerical values in a graphical manner.

Table 4. Trends Analysis Table—Level of Concern

Average ~ Concern 1–10					
	-5 Years	**Today**	**+5 Years**	**+10 Years**	**Concern 1–10**
State of Economy					7.7
Consolidation					6.3
Standardization of Tech					7.7
Reliability of Cloud					10.0
Mobility					7.4
Outsourcing					6.4
Security of Cloud					10.0
Political Ramifications					7.4
Avail of Shared Resources					6.0
Personnel Oversight					5.4

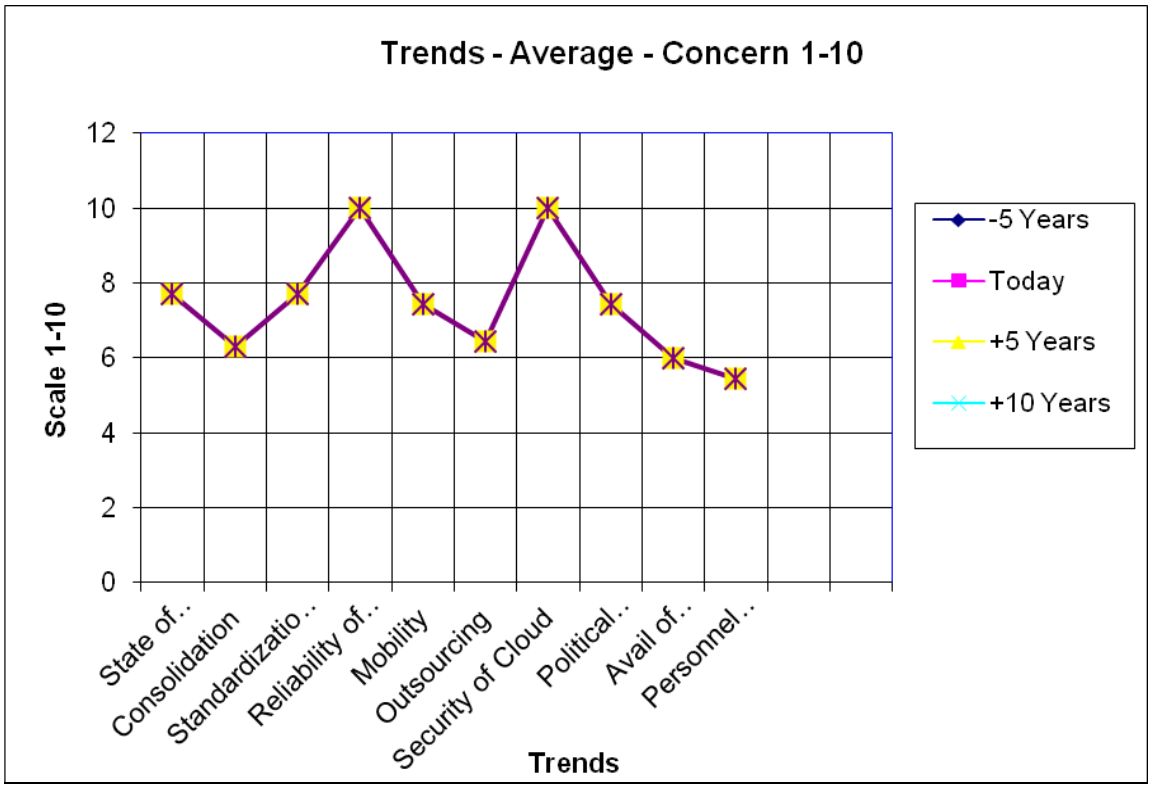

Figure 4. Trend Analysis Table—Level of Concern

C. EVENTS

An event is a significant occurrence or happening that takes place, which can have an impact, either positive or negative, on the identified issue. Unlike trends, events occur on a specific date or at a specific time and are usually singular occurrences. Trends are often described as unambiguous and confirmable.

Once the events were selected, all panelists individually rated them on four different criteria. Initially, the panelists projected the first year when they felt the event had a 1% chance of occurring. Secondly, they were asked to estimate the event's probability of occurrence, as a percentage, by assigning a value between 0 and 100% for five years (+5) and 10 years (+10) in the future. Finally, the panelists were asked to identify the impact of each event by assigning a numerical value between -10 and +10, with the highest positive number indicating the greatest impact.

Table 5 provides an example of the probability projection and level of impact for two events. In the example, Event #1 is perceived to be initially possible in three years. The example shows the probability of Event #1 increasing to 50% in five years and becoming a near certainty, or 100%, at ten years. This table also indicates that Event #2 is projected to have its first possibility of occurrence in seven years, making Event #2's occurrence in five years a 0% probability. However, in 10 years, Event #2 has a 10% probability of occurrence.

Table 5. Sample Event – Probability Projection and Level of Impact

Event	**Years >0 (1st year possible)**	**+5 Yrs (Future)**	**+10 Yrs (Future)**	**Impact (-10 to +10)**
Event #1	3	50%	100%	**-8**
Event #2	7	0	10%	**+8**

The impact of Event #1 in this table is rated -8. This number is interpreted to mean that the event has very little impact on the issue being discussed. On the other hand, Event #2 is rated as having a significant impact, with an assigned value of +8.

- 2011 NGT Results—Results

During this portion of the NGT, the panelists identified a total of 24 potential events. The process for documenting all of the events and ultimately selecting the top ten events was conducted in the same manner as with the trends. Once all of those ratings were completed, they were collected and entered into a spreadsheet. The average estimates were determined and the numbers were charted in the Table 6.

Table 6. Event Summary Table

Identified Events	Years >0	+5 Years (Future)	+10 Years (Future)	Impact (-10 to +10)
E1 = Budget Cuts	1.0	92.1	85.0	**0.4**
E2 = Unfunded Mandates	1.0	97.9	99.3	**-3.9**
E3 = Natural Disaster	2.7	75.7	85.7	**0.5**
E4 = Targeted Network Outage	2.7	58.6	74.3	**-2.3**
E5 = Legislative Mandates	1.3	77.1	147.1	**2.0**
E6 = Change in Political Leadership	2.0	100	100	**-0.9**
E7 = Decision to Privatize or Outsource	4.8	38.6	51.4	**2.0**
E8 = Implementation of NG-9-1-1	2.4	88.6	97.9	**6.9**
E9 = Consolidation of Government Agencies	3.0	55.0	62.9	**4.1**
E10 = Elimination of State Services	3.4	48.6	53.6	**1.7**

Event 1 = Budget Cuts

Although every member of the panel saw the timeline for when this event could occur as immediate, in light of our current economy, they varied greatly on the level of impact. During the discussion, members explained why they were at opposite ends of the scale. Some felt that the economic climate requires the use of “band-aids” and therefore, the implementation of a cloud-based system would be crippled. However, others had an

opposite perspective and said that the economy could drive the transition because all systems will fail eventually and the use of a cloud-based system may ultimately prove to be less expensive in the long run.

Event 2 = Unfunded Mandates

The panel largely agreed that unfunded mandates would often take away from the discretionary spending allocated to a project that is not mandated. Unless transition to cloud-based systems was mandated, agencies would like be forced to table the migration until suitable funding was available and not being used to implement other unfunded and mandated programs.

Event 3 = Natural Disaster

Some panel members felt that a natural disaster may push you away from moving to a cloud-based system, because a loss of connectivity to the cloud would likely occur. Therefore, the argument exists that traditional server-based systems are more reliable during a natural disaster, especially if you have the means to manipulate the equipment and restore service more rapidly. All agreed that a model that employs cloud-based technology, coupled with redundant local servers, would be a potential solution in order to overcome this type of hurdle.

Event 4 = Targeted Network Outage

Most panelists saw the targeted network outage as an event that would be devastating. However, the network security consultant certainly had the strongest views about this issue because he sees the number of attempts that currently occur on a daily basis. Most others have no idea how frequent and/or common these attempted intrusions happen.

Event 5 = Legislative Mandates

As the panel discussed legislative mandates, the conversation cited the mandatory migration to P-25 compliant radio systems as a mandate by the Federal Communications Commission. Fortunately, the implementation time line was more than five years, which provided time for agencies to react, however, the early years was spent finding ways to

acquire funding for the new equipment and the necessary re-banding that had to occur. Depending on the mandate and the amount of time provided for implementation, a legislative mandate can be disastrous, or inconsequential.

Event 6 = Change in Political Leadership

As we have seen throughout the years, a change in political leadership often results in changes to the priorities established by the previous administration. Whether at the executive level in our nation's capitol or more localized within state government, the fact remains that political agendas and priorities exist and funding is significantly impacted when priorities change. This can be a positive or negative change.

Event 7 = Decision to Privatize or Outsource

If the decision was made to outsource dispatch services, then the likelihood that we would migrate to the cloud is great. For an outside entity to assume responsibility of these services, their initial cost would be much less if they used a cloud-based platform. However, security concerns and the familiarity with a local dispatcher were two overarching negative issues that were raised when discussing outsourcing and privatization.

Event 8 = Implementation of NG-9-1-1

Of the ten events selected, implementation of Next Generation 9-1-1 clearly had the highest positive impact on the issue. Because of the technology associated with NG-9-1-1, the amount of data available to communications centers will increase drastically, thereby affording many more possibilities and options of how dispatch services are provided.

Event 9 = Consolidation of Government Agencies

Another event that the panelists felt would have a fairly positive impact on the consolidation of communications centers and the use of cloud-based technologies is the consolidation of government agencies. As the number of entities diminishes, there may be more public safety personnel that require dispatch services in outlying areas. For example, if another absorbs a small law enforcement agency, their dispatch center may be

eliminated, but the personnel performing law enforcement functions would still exist and require dispatch services.

Event 10 = Elimination of Services

If the decision is made to eliminate support services, such as the agency that hosts and maintains the radio system infrastructure, a void will be created and qualified technicians will no longer be available. That would force users to a different platform that could be maintained by an outside vendor.

Table 7 synthesizes the average numerical probability projection assessed by the panelists. A change in political leadership and unfunded mandates represent the two events with the greatest likelihood to occur in five years. Similarly, legislative mandates and a change in political leadership were seen as the most probable events that could impact implementation of emerging technologies ten years in the future. Figure 5 depicts the numerical values contained in Table 7 in a graphical manner.

Table 7. Events Analysis Table—Probability Projection

Average ~ +5/+10 Years				
	Years > 0	**+5 Years**	**+10 Years**	**Impact -10 to +10**
Budget Cuts		92.1	85.0	
Unfunded Mandates		97.9	99.3	
Natural Disaster		75.7	85.7	
Targeted Network Outage		58.6	74.3	
Legislative Mandates		77.1	147.1	
Change in Political Leadership		100.0	100.0	
Outsourcing		38.6	51.4	
NG9-1-1 Implementation		88.6	97.9	
Consolidation of Agencies		55.0	62.9	
Elimination of Services		48.6	53.6	

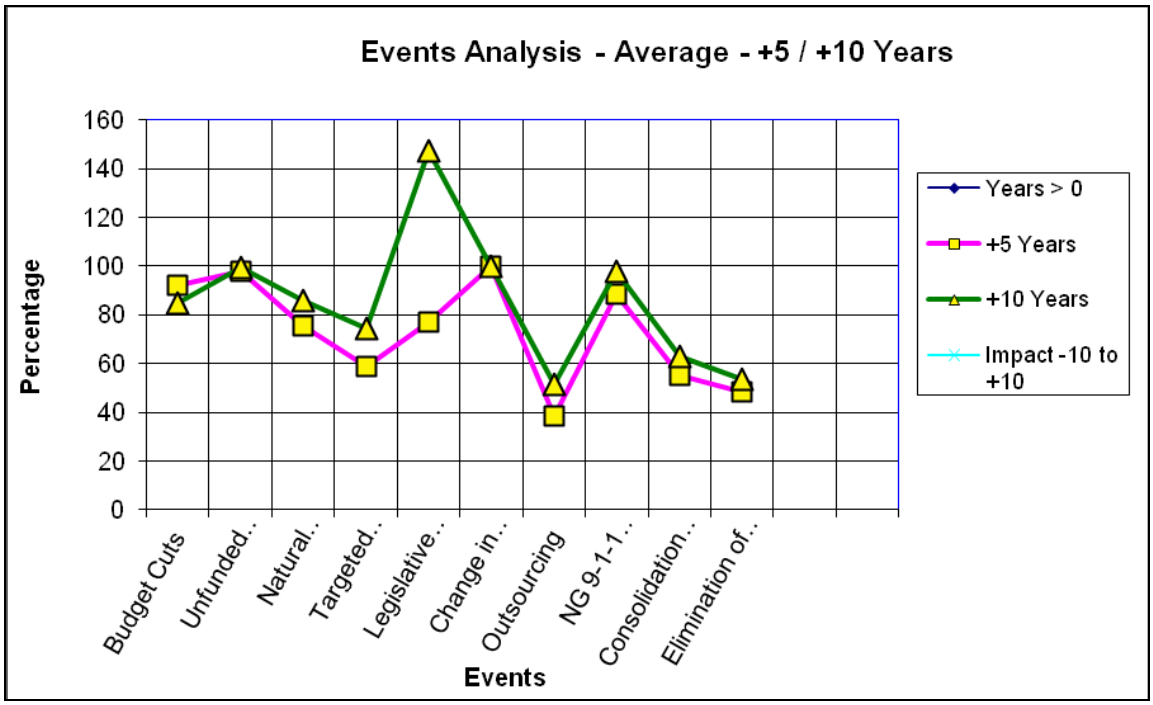

Figure 5. Event Analysis Graph—Probability Projection

Table 8 identifies the average level of impact each event would potentially have on the implementation of emerging technologies. The panelists identified the implementation of NG 9-1-1 as the most impactful event, closely followed by the requirement to outsource services. Figure 6 depicts the numerical values contained in Table 7 in a graphical manner.

Table 8. Events Analysis Table—Level of Impact

Median ~ Impact -10 to + 10				
	Years > 0	**+5 Years**	**+10 Years**	**Impact -10 to +10**
Budget Cuts				4
Unfunded Mandates				-5
Natural Disaster				0
Targeted Network Outage				-2
Legislative Mandates				1
Change in Political Leadership				-1
Outsourcing				6
NG9-1-1 Implementation				8
Consolidation of Agencies				7
Elimination of Services				1

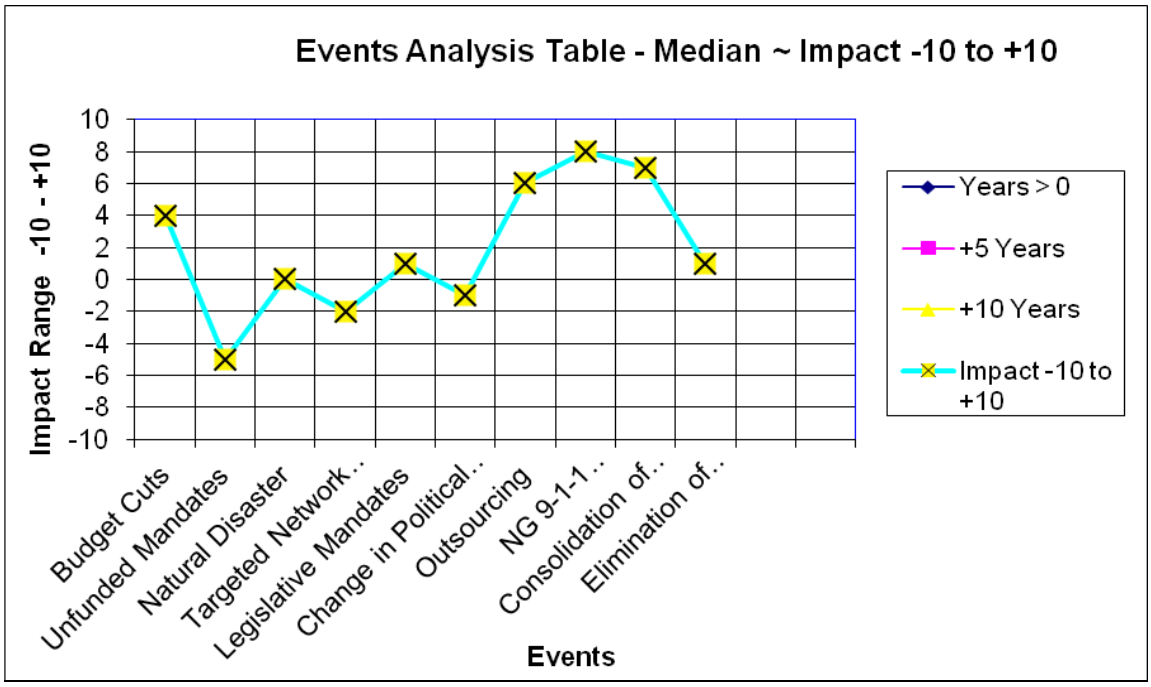

Figure 6. Event Analysis Graph—Level of Impact

D. CIA #1

The listing of identified trends and events is important, especially when their level of importance is weighted at a variety of times on a multi-year timeline. In this case, the 15-year range allowed the NGT panelist to use his or her knowledge base of past and present experience to estimate the future value of each trend and event.

The cross impact method is an analytical approach to the probabilities of an item in a forecasted set—in this case, the NGT trends and events.[33] Since we know that most events and trends are in some way related to others, a researcher can use their expertise to evaluate the potential interactions among the variables. The ability to understand and document such interactions proves to be valuable in many situations, especially decision making and prioritizing.[34] While often done in groups, "individual experts may estimate the probabilities."[35] The CIA is a quick and effective process that can help to understand the correlation between the two variables.

In May 2011, several weeks after the NGT exercise was completed, two police administrators we asked to complete a CIA using the events and trends generated by the original NGT group. The CIA table highlights the panel's assessment of the impact of each event on each trend. For this exercise, the panel members were instructed to use the range of -5 to +5, with zero reflecting no impact. A lesser value, such as -5, represents the panel's opinion that it would be less likely that the event would impact the trend, whereas a value of 5 indicates that the event would have the most significant impact on that trend. The results of their analysis are highlighted in the CIA table.

This CIA captured a snapshot of what impact each event would have on the trend listed. The background of each evaluator, coupled with the interpretation of the environmental factors present during that time clearly influenced the rankings applied to each relationship. Over time, those influences will likely change, as will the

[33] Gordon, "Cross-Impact Method."

[34] The Vision Center for Futures Creation, "Trend Analysis."

[35] Gordon, "Cross-Impact Method."

interpretations of varying evaluators. With that in mind, this portion of the analysis is highly subjective.

Table 9 depicts the CIA of each event on each trend from the initial panel. A narrative analysis of the panel's discussion is provided for the five most significant relationships.

Table 9. 2011 CIA Significance Rating Table

	T1 = State of the Economy - Fiscal	T2 = Consolidation of Resources	T3 = Standardization of Technologies	T4 = Reliability of the Cloud	T5 = Mobility	T6 = Outsourcing	T7 = Security with the Cloud	T8 = Political Ramifications	T9 = Availability of Shared Resources	T10 = Personnel Oversight
E1 = Budget Cuts	0	5	3	1	1	3	1	3	4	2
E2 = Unfunded Mandates	-4	4	4	1	2	3	1	3	3	1
E3 = Natural Disaster	-2	4	2	2	4	2	1	1	4	1
E4 = Targeted Network Outage	1	2	2	3	3	2	5	0	1	1
E5 = Legislative Mandates	4	2	3	1	1	2	1	1	2	1
E6 = Change in Political Leadership	3	2	0	0	0	2	0	1	3	0
E7 = Decision to Privatize or Outsource	3	3	2	4	-3	0	3	-2	-2	-4
E8 = Implementation of NG-9-1-1	1	2	5	0	3	1	0	1	4	1
E9 = Consolidation of Government Agencies	3	3	2	1	1	3	1	5	5	2
E10 = Elimination of State Services	1	2	2	2	1	4	2	-3	3	1

1. The Impact of Event #1 (Budget Cuts) on Trend #2 (Consolidation of Resources)

The panel felt that budget cuts (Event #1) was likely to have the most significant correlation of the decision to consolidate resources (Trend #2) among public safety communications centers. At the time of the CIA, the state of California was enduring some of the toughest budgets times in nearly fifty years. Agencies across the state were looking for creative ways to survive the fiscal crisis and they were preparing for the worst—to include laying off significant numbers of personnel. As a result, consolidating resources with other public safety providers was a common discussion among department heads. Although the trend did not include many communications centers, creating regionalized teams for services, such as Special Weapons and Tactics (SWAT), explosive ordnance detection (EOD), etc., became quite common. Their rating of +5 is consistent with the pressure and concern they were faced with when this analysis was conducted. With less money available to agencies, they were forced to explore ways to save the valuable dollars they had.

2. The Impact of Event #4 (Targeted Network Outage) on Trend #7 (Security with the Cloud)

A targeted network outage, or some form of cyber attack, would likely test the security of the cloud-based system. Granted, a network attack may also impact a traditional server-based system, however, many feel that it is easier to control and/or mitigate a localized attack. In either case, the panelists felt that there was tremendous correlation between the security of the cloud and a targeted network outage.

3. The Impact of Event #7 (Decision to Privatize or Outsource) on Trend #10 (Personnel Oversight)

This was the only cross impact with a significantly negative impact. Many law enforcement managers feel a sense of control when they can have direct oversight of an employee. Should the decision to privatize or outsource occur, this ability would be removed from the law enforcement manager, as the personnel would no longer be employees of the organization. Recognizing that the panelists were law enforcement managers, it is not surprising that they found this to be a very negative prospect.

4. The Impact of Event #8 (Implementation of NG-9-1-1) on Trend #3 (Standardization of Technologies)

Implementation of NG9-1-1 will benefit law enforcement because the technology associated with NG-9-1-1, will drastically increase the amount of data available to communications centers, thereby affording many more possibilities and options of how dispatch services are provided. There is obviously a positive a correlation between this event and trend.

5. The Impact of Event #9 (Consolidation of Government Agencies) on Trend #9 (Availability of Shared Resources)

The panelists felt that as government agencies are forced to consolidate, the amount of resources available will likely increase. When the researcher discussed this with them after they completed their analysis, they used the following example. If Agency A has ten specialized teams and Agency B has six different specialized teams, they now have 16 specialized teams between them.

III. ANALYSIS OF KEY ISSUES

As identified in the original NGT exercise, several trends and events were identified. The events were evaluated using criteria, including the probability of the event occurring five years in the future and ten years in the future and the degree of impact the event would have on the issue if it were to occur. Similarly, the trends were judged on their perceived "level of impact" five years in the past, the projected "level of impact" the trend would have on the issue five years in the future and ten years in the future. Lastly, the trends were assessed a numerical a "level of concern" rating from 1–10. Although five years have not elapsed since the original NGT, looking at the projections to determine if they are trending in the direction originally anticipated can provide a glimpse into the accuracy of the initial projection.

The original trend analysis table (Table 10) depicted that the reliability of the cloud was one of the most concerning issues among the panel members. Recognizing that many technological systems would likely evolve into cloud-based platforms over the next five to ten years, the reliability of the cloud infrastructure was deemed critical. Similarly, the panel concluded that the ability to move operations from one place to another was a very attractive option, especially if it could be done quickly and seamlessly. Not only would this be beneficial during emergency incidents or large-scale events, but it would be advantageous when trying to maintain reasonable call volumes, or when attempting to circumvent a system outage affecting the local carrier. Mobility, as it was described, becomes a viable option as a result of the possibilities created by cloud-based systems. The third most significant trend projected for five years in the future was the security of the cloud. Similar to the reliability of the cloud, the security of the data residing in cyberspace was seen as a critically important trend. With a limited number of cloud users five years prior to the NGT, the level of impact was minimal, however, as more and more users began migrating to cloud-based systems, security concerns were projected to increase rapidly.

Table 10. Trends Analysis Table

	-5 Years	+5 Years	+10 Years
State of Economy	91	135	154
Consolidation	56	133	134
Standardization of Tech	65	146	159
Reliability of Cloud	22	175	186
Mobility	61	166	186
Outsourcing	40	131	153
Security of Cloud	44	161	179
Political Ramifications	68	125	150
Avail of Shared Resources	58	153	181
Personnel Oversight	62	114	130

A. CIA #2

The initial CIA captured a snapshot of what impact each event would have on the trend listed. The background of each evaluator, coupled with the interpretation of the environmental factors present during that time clearly influenced the rankings applied to each relationship. Those environmental influences may still exist three years later, or there may be more significant factors that have caused an increased level of concern. Similarly, there may be influences that have subsided over the past 33 months, which would likely result in a reduction of their perceived impact on the trend listed. For the purposes of the second CIA, the researcher evaluated the original events and trends and conducted a second CIA in January 2014 (Table 11).

Table 11. 2014 CIA Significance Rating Table

	T1 = State of the Economy - Fiscal	T2 = Consolidation of Resources	T3 = Standardization of Technologies	T4 = Reliability of the Cloud	T5 = Mobility	T6 = Outsourcing	T7 = Security with the Cloud	T8 = Political Ramifications	T9 = Availability of Shared Resources	T10 = Personnel Oversight
E1 = Budget Cuts	0	4	-1	0	0	1	0	2	4	-1
E2 = Unfunded Mandates	-1	2	3	0	1	2	0	1	1	0
E3 = Natural Disaster	0	4	2	4	4	-1	0	1	3	-1
E4 = Targeted Network Outage	2	1	0	5	3	-1	5	5	3	-1
E5 = Legislative Mandates	4	-1	4	5	0	2	5	0	2	0
E6 = Change in Political Leadership	0	1	0	0	0	1	0	0	1	0
E7 = Decision to Privatize or Outsource	3	2	0	3	0	0	4	1	0	-3
E8 = Implementation of NG-9-1-1	3	3	5	4	3	2	4	0	3	0
E9 = Consolidation of Government Agencies	3	3	1	0	2	2	0	4	4	3

B. COMPARISON OF CROSS IMPACT ANALYSES

A comparison of the 2011 CIA and the 2014 CIA reveals a shift in the level of correlation between several events and trends. Two events, the implementation of Next Generation 9-1-1 and a targeted network outage remained highly significant, with a targeted network outage seeing an expanded correlation to additional trends. The graph below depicts the difference between the values assessed in the 2011 CIA versus the

2014 CIA. There are several relationships not noted in Figure 7 that are discussed in the analysis below, as their values were high in 2011 and in 2014, so they did not reflect a significant difference on the graph.

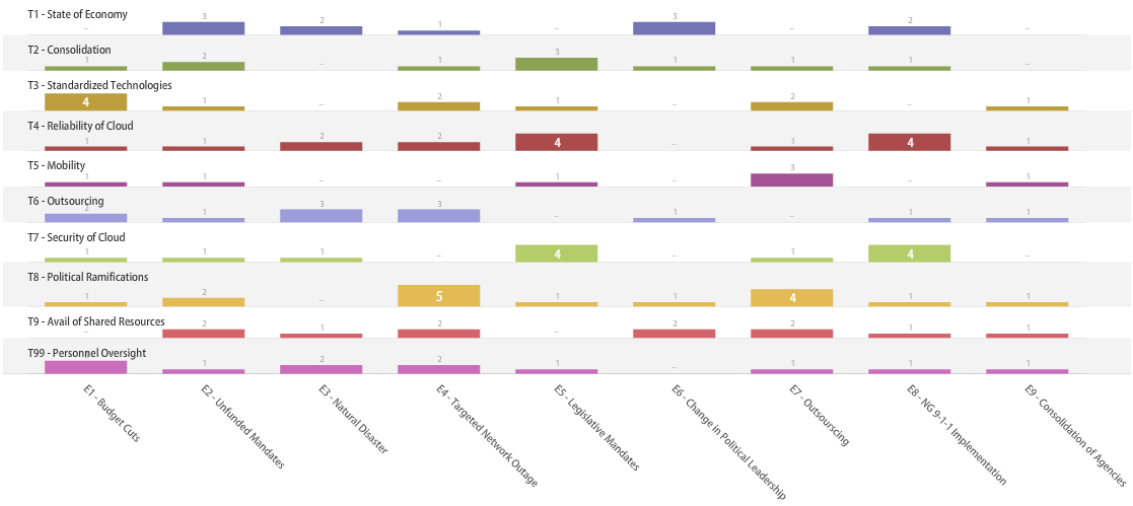

Figure 7. Comparison of 2011 and 2014 CIA Significance Ratings

1. Analysis of Event #4

Targeted Network Outage/Security: In the 2014 CIA, the relationship of one event (Event #4—Targeted Network Outage) was estimated to have a considerable impact on three trends. Those trends included Trend #4—Reliability of the Cloud, Trend #7—Security of the Cloud, and Trend #8—Political Ramifications. There were no other events with such a significant correlation to as many trends.

A "targeted network outage," which can be loosely described as any type of intentional disruption to the system, whether cloud-based or traditional, was originally linked to "security of the cloud" and given the maximum value of 5. In the most recent CIA, the same value was assessed and the correlation with "reliability of the cloud" and "political ramifications" also increased to the maximum value of 5.

With increasing reliance on cloud-based networks, a targeted network outage, or some form of cyber attack, would likely have a significant impact on the ability of governments and the public to conduct their business in the manner that they have

become accustomed to. A targeted network outage, or some form of cyber attack, would likely test the security of the cloud-based system. There is a tremendous correlation between the security of the cloud and a targeted network outage, as the value of the information stored in cloud-based servers is becoming increasing important. Furthermore, the volume of that data is expanding exponentially.

With the expanded proliferation of cloud-based technology and the seemingly increasing number of breaches of personally identifiable information, the public outcry has increased dramatically since the initial CIA. Although the data breaches do not constitute a "network outage," it is likely that with the ability to obtain information from the system, the offender would also have the ability to sabotage the system. Rather, such an action would immediately make their presence know and end their ability to gather as much personal data as possible. As an example, Edward Snowden's access to the National Security Administration (NSA) databases allowed him to extract approximately 1.7 million files over an extended period of time.[36] Had he chosen to disable the NSA systems at the beginning of his operation, the volume of data he would have been able to obtain would have been greatly reduced. The political ramifications associated with Snowden's actions have reached the highest levels of various governmental agencies.

Similarly, there are frequent instances of data breaches discussed in the mainstream media, a phenomenon that rarely occurred in 2011. The personal impact of such intrusions is being recognized by hundreds of millions of people at a time and again, the public sentiment is becoming increasingly more negative. Most recently, the Target Corporation notified its customers that a data breach occurred, wherein an estimated forty million customers had their personal data stolen. As the weeks progressed, the magnitude of the breach continued to expand, with Target admitting that personal identification numbers (PIN) had been stolen and gradually increasing the potential number of affected customers to over 110 million—nearly 1/3 of the population of the United States!

[36] Business Insider, "NSA: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them," accessed March 22, 2014, http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12.

As evidenced by the fallout from various compromises of data (both public and private) and the failure of critical systems (such as the 9-1-1 system on the east coast), it is evident that the involvement of public officials has become a significant concern.

Public and private clouds exist, and clearly, for law enforcement purposes, agency directors must ensure the clouds they utilize will maintain the integrity of the data stored there. In 2002, the federal government established the Federal FISMA, which established strict information security protocols.[37] Initially, many public safety agency directors felt physical control of their data was a necessity, meaning data servers must be at a secure location, such as their police station. The public sector, though, has embraced the need for secure cloud space and created specific segments that meet the FISMA standards, such as, Google Apps for Government, which provides segregated systems for U.S. government customers and the data is stored exclusively in the United States.[38]

In conjunction with FISMA, the development of appropriate security protocols must be developed to ensure that sensitive data cannot be compromised. In response, Federal Chief Information Officer Steven VanRoekel said in 2011 that the White House's Office of Management and Budget (OMB) would launch the FedRAMP, a unified government-wide risk management initiative focused on providing security for cloud-based systems. The program offers a standard approach to conduct security assessments of cloud systems based on an accepted set of baseline controls and consistent processes vetted and agreed upon by agencies across the federal government. He added, "as the government migrates to the cloud, we are committed to doing so in a way that is cost effective and ensures the safety, security and reliability of our data. To date, each federal agency has gone through multiple steps that take anywhere from six to 18 months and countless man hours to properly assess and authorize the security of a system before it grants authority to transition to the cloud."[39]

---

[37] *Wikipedia*, s.v., "Federal Information Security Management Act of 2002," accessed November 17, 2012, http://en.wikipedia.org/w/index.php?title=Federal_Information_Security_Management_Act_of_2002&oldid=480447665.

[38] "Security."

[39] Higgins, "Feds Aim to Lock Down the Cloud."

With that in mind, it is apparent that the level of support for cloud use is increasing and should continue to expand, provided appropriate levels of security are incorporated. In an interview with Nicholas Popp, vice president of product management and development at Symantec, he acknowledged the cloud is not quite up to par with on-premise installations when it comes to security. He predicted within three to five years, though, the cloud will be the more secure environment for small and mid-sized businesses.[40] Additionally, according to David McClure, associate administrator for the Office of Citizen Services and Innovative Technologies at the General Services Administration said, "FedRAMP will evolve as a program to reflect the changing nature of cloud computing and incorporate lessons learned. As cloud computing, standards and capabilities evolve, so will FedRAMP." McClure also noted that a joint authorization board (JAB) would be established to define and update FedRAMP security standards.[41] Cloud computing has the potential to play a major part in addressing inefficiencies in government, improving government service delivery, and saving money.

2. Analysis of Event #8

Implementation of NG9-1-1: Implementation of NG9-1-1 (Event #8) will benefit law enforcement because the technology associated with NG-9-1-1, will drastically increase the amount of data available to communications centers, thereby affording many more possibilities and options of how dispatch services are provided. In order for NG-9-1-1 to succeed, the platforms on which it will operate need to be consistent throughout the country. Therefore, its impact on the standardization of technologies (Trend #3) is significant.

The implementation of NG 9-1-1 and its impact on the standardization of technologies remained consistent over the three years in between the CIA analyses. In 2011, NG-9-1-1 was on the minds of industry leaders; however, the overarching impact of the new platform was not clear to many people. Over the past three years, the clarity of the NG-9-1-1 system has improved dramatically, with limited implementation thus far.

[40] Olavsrud, "Security in the Cloud Is All About Visibility and Control."

[41] Higgins, "Feds Aim to Lock Down the Cloud."

With some agencies taking the first step, now handling text-to-911, it is evident that the industry is getting closer to full-scale implementation of NG-9-1-1. The information technology manufacturers are working to create their new platforms in accordance with the parameters that are being designed and developed by the governmental agencies responsible for the creation of the new NG-9-1-1 network. Therefore, the potential impact of NG-9-1-1 on the standardization of technology is one of the greatest correlations.

3. Analysis of Event #5

Legislative Mandates: In 2011, one impact that was previously ranked as "near null" was the impact of legislative mandates on the reliability and security of the cloud. However, with the introduction of the federal government's "cloud-first" policy, federal agencies must first try to incorporate some type of cloud computing into each IT project under consideration.[42] This mandate will likely drive improvements in the reliability and security of the cloud, especially if sensitive or critical data and programs will reside there.

As policies are created or modified, particularly those that mandate inclusion of cloud-based applications and data storage, the required reliability and security of the cloud infrastructure also increase. Legislative Mandates often drive the direction of an agency. Frequently, compliance with such mandates determines whether an agency will qualify for programs or funding.

4. Analysis of Event #9

Consolidation: In 2011 the consolidation of agencies was a common theme in government and public safety as a result of the budget crisis impacting most departments. As a result of a dismal fiscal outlook and no light at the end of the tunnel, small-scale consolidations began occurring among specialized teams and units, such as EOD teams, special weapons and tactics teams, etc. Those early consolidations led to discussions regarding larger scale opportunities, including full-scale agency consolidation or partial consolidation, including communications centers. The availability of shared resources could provide an opportunity for several agencies to band together in order to save

[42] Federal Computer Week, "When the Cloud Makes Sense."

personnel costs, while committing to only maintain one facility and the infrastructure therein. As the financial outlook has started to improve, the rush to consolidate has subsided. Although some agencies are still exploring the opportunities, the political emphasis placed on agency executives and communications center directors to consider consolidation has diminished.

Throughout the public safety community, officers and dispatchers often share a unique relationship because of the situations that they encounter. Officers often credit dispatchers with assisting them in the mitigation of a particularly sensitive call for service. There is a long-standing belief amongst the law enforcement community that there is value in having dispatchers who are located within a reasonably close proximity to those to whom they provide dispatch services. Public safety agencies may lose that "personal" connection to their communications center; rather, a consolidated model may cause a shift from communications centers with dispatchers who are known to the field personnel to an entity that simply provides a delivered service. For those agencies located in high cost of living areas, consolidating or outsourcing services to a more reasonable location could provide additional cost savings. Lastly, for agencies maintaining more than one communications center, consolidation may provide an avenue for significant reduction in expenditures. Infrastructure costs of both the physical facility, as well as the ongoing cost of upgrading and maintaining the computer equipment are significant. Reducing the overall number of facilities would be a method to decrease that cost tremendously.

Consolidation comes with a host of collateral issues. One of the key issues, which is an area rich for future research, is the human/personnel element associated with consolidation. This is further detailed in Chapter VI.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DISCUSSION

A. FINDINGS

The completion of the NGT exercise, as well as the two CIAs provide excellent insight as to what challenges may be on the horizon for public safety leaders. The convergence of the identified events and trends will likely drive the future of public safety communications centers. The ability to forecast and prepare for those situations can provide an agency with a distinct advantage over their ill-prepared colleagues. The following trends and events identified by the initial NGT panel were determined to be more "significant" than the others and therefore, will likely be important factors to consider when assessing our level of readiness for the introduction of emerging technologies.

- Trend #4 (Reliability of the Cloud)
- Trend #7 (Security of the Cloud)
- Trend #8 (Political Ramifications)
- Event #8 (Implementation of NG-9-1-1)
- Event #9 (Consolidation of Government Agencies)

Reliability is one of the most prominent concerns associated with cloud-based system. One cloud-based platform involves contracting with a third party to provide a "hosted" or "managed" solution. As a part of the contract with that vendor, there would likely be a guarantee that no critical communications will be interrupted, because should the primary system fail, or be taken off-line for maintenance, the secondary data stream will ensure there is no interruption. However, what happens if there is an interruption? Is there an acceptable level of "down-time?" The 9-1-1 system has seen significant failures throughout the country and it has been attributed to weather or a phone company problem. On June 29, 2012, a significant storm caused a multi-day outage to over 2.3 million customers in the Washington, DC area. There were no significant sanctions levied against the telephone provider, although Verizon and Arlington County agreed to

improve the redundancy in their systems.[43] If a cloud-based system is being managed by a third party and a failure occurs, will they be sanctioned? That answer is yet to be seen.

NG9-1-1 is still in its initial deployment stage and many aspects are still being finalized. However, it has become clear that NG9-1-1 will dramatically change the landscape of 9-1-1 call answering as we know it today. Once implemented, the NG9-1-1 system will likely allow

- quicker and more accurate information delivery to responders
- better and more useful forms of information (data, images, and video)
- more flexible, secure and robust PSAP operations
- lower public capital and operating costs for emergency communication services
- ability to seamlessly route overflow calls to other PSAPs
- improved routing of calls, based upon location and status of the PSAP
- ability to isolate calls from a specific incident (based upon location) and queue those calls separately from all incoming 911 calls
- ability to transfer calls from one PSAP to another along with the associated location data, call-taker notes, text/video/pictures, etc.
- enhanced reporting capabilities

One of the key potential applications of NG9-1-1 is data sharing between agencies, based upon outlined rules and memorandums of understanding (MOUs). This shared data may include

- hazardous materials information
- building plans
- medical information
- prior responses to a specific address
- geographical information systems (GIS) data

[43] Andy Smith, "Derecho 911 Problems Lead to Changes from Verizon, Arlington County (#DMVReads)," *The Washington Post—Blogs*, August 20, 2012, http://www.washingtonpost.com/blogs/the-buzz/post/derecho-911-problems-lead-to-changes-from-verizon-arlington-county-dmvreads/2012/08/20/eecb31b2-eade-11e1-b811-09036bcb182b_blog.html.

B. IMPLEMENTATION

1. Scenario Planning

Scenario development is a tool designed to assist organizational leaders and decision makers in identifying how identified trends and events may possibly create problems, challenges and opportunities that the future would present. The process of scenario development has been utilized in the past and is a valuable tool when attempting to devise a strategy for moving forward.[44] What is important for the reader to remember is a scenario is not a specific forecast of the future, but a plausible description of what might happen. Using the events and trends developed during the Nominal Group Technique exercises; two scenario examples were created in order to depict the role of integrating emerging technologies and cloud-based solutions into public safety communications centers. Additionally, by identifying some of the potential barriers and mitigation steps, these scenarios can assist public safety leaders in achieving a successful implementation.

a. Probable Scenario

When the new Governor came into power after the 2015 recall election, he immediately reinstated all funding previously cut over the past ten years (Event #6). For the state's law enforcement services department, this meant a baseline increase of approximately $420 million (Trend #1).

Although the past ten years were quite difficult, the department managed to survive an unprecedented period where personnel numbers were slashed, purchases deferred for years at a time, infrastructure was allowed to suffer and the necessary technological advancements were ignored in order to simply survive. The question now, was how to allocate a windfall of money in order to get back on track (Event #1).

The department decided that a new computerized data system for all communications centers and patrol vehicles would be an excellent expenditure. The magnitude of a project that size would be enormous, however, with the ability to hire

[44] Gilmore Commission Report, *Forging America's New Normalcy: Securing Our Homeland Preserving Our Security*, vol. Five (Arlington, VA: RAND Corporation, December 15, 2003), 11–20.

endless personnel in order to implement the system, perhaps it would be possible. The thought of snazzy new computers tied to GPS tracking modems in every car, a robust Computer Aided Dispatch system and the incorporation of NG9-1-1 technology (Event #8) with recent advancements in GIS would surely make the new system the envy of every agency.

As the word began to spread, many law enforcement agencies asked the department to take over their dispatch functions because they realized that they would never have the funding that the department was enjoying. Some small agencies felt that even if they received funding, they were so far behind the curve; they would never be able to complete a wholesale replacement of their current system. In the end, more than half of the law enforcement agencies partnered with the department as massive regional dispatch centers were built throughout the state (Event #9/Trend #2).

Through mergers with other agencies, the equipment used became far more standardized and field officers enjoyed common platforms with other agencies (Trend #3). This allowed for more successful integration and information sharing. In the end, the ability to transmit data from one police car to an allied agency patrol unit was almost seamless. Of course, this technology did not come cheap. In a five-year period, the department spent nearly $3 billion on equipment, consultants and technicians in order to implement the "perfect system."

b. Preferable Scenario

The state's law enforcement department has embarked upon a sweeping change in the realm of public safety dispatching. Because they were exempted from the crippling restrictions of the state procurement system, they were able to competitively bid a new dispatch model to a world-renowned vendor. The vendor will provide the technology and infrastructure for three consolidated dispatch centers throughout the state. Each will be equipped with state-of-the-art computer systems that operate on cloud-based technology (Trend #4/Trend #7), keeping infrastructure costs to a minimum and saving millions of dollars in software and information technology expenses. Although many IT positions will no longer be needed to support the dispatch center infrastructure, those employees

will be redeployed within the agency to handle other IT-related needs. Furthermore, the operating cost for three locations, rather than the 25 centers previously maintained by the department should be nearly $20 million dollars less each year and the ability to effectively manage personnel in three locations rather than 25 will be much greater (Trend #10).

As the geographic locations for each of the new facilities was debated, current employees quickly rallied behind several of the initial choices. At the onset, fears of mutiny surfaced because the dispatchers were known for their abrasive personalities and their unwillingness to work with the department and its managers. However, many felt that a location in the northern part of the state, one in the middle and a third near the southern border, would afford people a variety of options. Additionally, because of the anticipated annual savings, the department agreed to cover the moving expenses of all affected dispatchers and to assist with the closing costs of their new residences.

Shortly after construction was complete at two of the three facilities, it became evident that working conditions were remarkably improved, thereby leading to much-improved service delivery and employee well being. Several software updates have already been implemented and the cost to the department has been non-existent since a three-year upgrade provision was included in the initial contract. In the end, it appears that only a small portion of funding earmarked for a complete overhaul of the public safety dispatch centers will be needed. Through the use of truly competitive bidding, the residents of the state will save a significant amount of money each year and receive the best dispatch service available in the open market.

Scenarios are not meant to be factual, nor are they intended to show what will happen in the future. Rather, they are intended to broaden the horizons and expand the imagination of the researcher. The road map of the future will have a variety of possible routes. Ultimately, it will be up to the researcher to determine which route is best and then execute the plan, leading the group into the future.

2. Strategic Planning

Successful corporations, whether private, public or governmental, maintain an accurate "road map" in order to guide them in executing their global vision. Public safety agencies should conduct regular assessments of their operations and implement goals and strategies aimed at improving their operations. When integrated, the assessments, "road map," and vision can be woven together to create a well thought-out strategic plan.

Preparing for a world in which the public expects instant access to law enforcement dispatch services requires long and short-term planning. Strategic planning fills the void between the present and the near-distant future (10 to 20 years). Strategic planning provides an operational framework for organizations looking to do more than merely react to the world around them. A well-formulated strategic plan will include a development team that is representative of key stakeholders and interest groups and should prepare an agency for the challenges it faces tomorrow while laying the foundation for addressing issues down the road.

There are several strategic planning models available for use by public sector agencies, one of which is the Bryson Model. The Bryson Model is described and presented, in the author's book *Creating and Implementing You Strategic Plan—A Workbook for Public and Nonprofit Organizations.*[45]

Like other strategic planning models, the Bryson Model begins by assessing an organization's readiness for creating, adopting and, most importantly, implementing a strategic plan. This assessment is followed by an internal and external environmental scan; an identification of strategic issues facing the organization; the formulation of strategies to address these issues; the review and adoption of the plan; the establishment of an organizational vision; the development of an implementation plan; and, a periodic review, assessment and adjustment of the plan over time.

The strategic plan of a public safety agency will likely represent a five-year strategy for addressing the identified goals and moving them affirmatively toward the

[45] Farnum Alston and John Bryson, *Creating and Implementing Your Strategic Plan—A Workbook for Public and Nonprofit Organizations* (San Francisco, CA: Jossey-Bass, 2005).

agency director's vision. A team, led by an experienced manager, normally manages the planning effort. This strategic planning coordination committee will carry out the following steps in the creation of the plan: 1) reviewing the previous plan (if one exists) and assessing the successes and failures in its implementation, 2) identifying the key internal and external stakeholders and determining their role in the process, 3) conducting an environmental scan and identify the most pressing or urgent issues to be addressed in the plan, 4) agreeing upon the goals and objectives to pursue over the life of the plan, 5) developing the action steps and performance measures for the goals and objectives, 6) developing or agreeing upon a reporting method and frequency, and 7) reviewing the plan at least annually for any necessary adjustments.

An effective strategic plan is a living document in which progress is tracked and documented, with the plan being adjusted as needed. Quarterly reporting by internal stakeholders documents progress on their action steps. An annual report will be prepared that consolidates quarterly reports from all stakeholders and assesses and documents the overall effectiveness of the plan in meeting its goals and objectives. The strategic planning coordinating committee should monitor quarterly stakeholder reports and prepare the consolidated annual report.

a. Organizational Mandates

A law enforcement agency is required to provide general law enforcement services to all individuals and entities within its geographic boundaries. These responsibilities are carried out through proactive patrol in public areas, apprehension and arrest for crimes as defined by state law or appropriate local ordinance and traffic enforcement on public roadways. Numerous investigative and administrative duties support these general requirements. The chief of police also has administrative and procedural responsibilities that facilitate the day-to-day management of the department and long range planning for the department specifically and city government as a whole.

Effective delivery of the services listed above requires the police department to maintain various methods of communication with its constituents. Citizens requesting law enforcement services need to know how and under what circumstances they should

use a wired or wireless phone, the Internet, written correspondence or face-to-face communications. The department's responsibility is to provide as many reasonable avenues for communication as its resources will bear. 9-1-1 telephone services are universal throughout the United States and also exist in various forms in the majority of countries around the globe. The requirement to answer 9-1-1 calls (including providing the staffing, equipment and infrastructure) is contained in state statute and, in many jurisdictions, is further clarified in local charters or other governing documentation. The police department has internal policies for managing the implementation of state and local requirements for processing 9-1-1 calls and providing programmatic support.

b. Stakeholders, Mission, Values and Vision

Effective delivery of the services listed above will require the agency to provide various avenues in which the public can interact with the department. In turn, dispatch personnel must be able to quickly respond to requests from the public, patrol officers, allied law enforcement agencies, and other stakeholders. Furthermore, the agency must create a secure infrastructure that will allow for seamless integration, advances in technology and mobility throughout the state.

A law enforcement agency's mission and mandates must support its purpose and role as a government entity. In order to justify its existence to its constituents, the department must create "social value."[46] A strong mission statement and set of organizational values provides a framework for establishing the organization's identity and is the foundation for its strategic plan. This same mission statement can serve as a source of motivation or inspiration for employees.

An effective strategic plan begins with a thorough assessment of the environment in which the department currently operates and future scenarios in which it may be operating within the next three to five years. Examining trends and plausible future events and constructing possible outcomes helped in the development the future scenarios depicted above. One environmental scanning model is the SWOC (strengths, weaknesses,

[46] Alston and Bryson, *Creating and Implementing Your Strategic Plan—A Workbook for Public and Nonprofit Organizations*.

opportunities and challenges) analysis. A scan of the internal and external environments for each of these categories will provide insight into the value the department currently brings to its constituents and sheds light on the effectiveness, or lack thereof, of the previous planning efforts in reaching its critical success factors.[47]

The creation of a well-formulated set of strategic issues depends upon the application of sound strategic planning principles. The issues facing most public safety agencies are common among large and small public safety departments throughout the country. Budget cuts due to prevailing economic conditions create challenges in maintaining a sufficient number of officers and support staff to accomplish the department's mission; aging equipment is not replaced when it reaches the end of its useful life; facilities, technology and communications infrastructure that should have been replaced years ago are moved to a lower priority and funding for community outreach or criminal apprehension programs has been eliminated. Similar economic challenges throughout the community as a whole are causing crime rates to increase and the general quality of life to decrease.

Another significant issue facing departments is the rapid evolution of communications technology and the methods in which officers, dispatchers and members of the public communicate with one another. An implementation solution for how to manage these emerging technologies is necessary in order to provide long-term solutions for public safety executives charting the future of their agencies.

Funding from local sources will be difficult, unless the economy improves early in the life of the plan and gives the city flexibility to increase funding to the department. The public safety agency should pursue federal funding made available to each state through the ENHANCE 9-1-1 Act of 2004. The Act makes $250,000,000 per year available for NG9-1-1 projects. The department should also revisit the formula for 9-1-1 fund distribution for PSAP to ensure every available dollar is being requested, received and used.

---

[47] Alston and Bryson, *Creating and Implementing Your Strategic Plan—A Workbook for Public and Nonprofit Organizations*.

Infrastructure strategies should address migration from public branch exchange (PBX) phone systems to a voice over VoIP system capable of supporting intelligent call routing, data and voice communications, interoperability and shared network services. The established procurement process may be the likely avenue for acquiring the upgraded 9-1-1 system, but some thought should be given to shared acquisition or leveraged procurement with other public safety answering points in the region. Sharing services or a purchasing vehicle could result in significant savings and possibly shorten the procurement cycle. Implementation planning can start once the project(s) is approved, funding identified and the procurement process starts. Execution of the plan, of course, is dependent upon the success of the predecessor activities.

As an example, transition to a cloud-based NG9-1-1 system will require a re-assessment of staffing formulas and job descriptions. Dispatch center business processes will undergo significant change with the introduction of text, video and picture processing. The nature of dispatcher and citizen interaction will be affected as well. Retraining to meet the requirements of NG9-1-1 service delivery will be a significant undertaking.

A comprehensive transitional program must also include public education on the type of services available and an explanation of what constitutes appropriate use of the system. Managing public expectations is important to the success of the program. If citizens expect a reply for every text, video or picture message sent and do not receive one, they will have a negative impression of the quality of service delivered by the department.

Specifically related to the consolidation of communications centers and the incorporation of cloud-based computing technology, the agency will need strategies that address funding, infrastructure, procurement and implementation, staffing, training and public information and education. While some strategies can be pursued simultaneously, others are sequential. This means that some strategies will be more time-bound and must be tracked diligently to ensure that they are not forgotten about or lose momentum because they cannot be started for a year or more.

Infrastructure strategies should address the use of emerging technological advancements, such as interactive GIS mapping applications, GPS location data, migration to a VoIP system capable of supporting intelligent call routing, data and voice communications, interoperability and shared network services, and the use of radio over Internet protocol (RoIP).

In doing so, a dispatcher may have the ability to answer a call for service from the public, summon emergency response personnel or other service providers, such as tow trucks or taxis, determine the location of all patrol units and dispatch the closest available unit from anywhere in the state. Communications center managers would be able to re-route dispatch traffic in the event of an emergency or when the volume has exceeded the capacity of the communications center, essentially "moving" the dispatch operations anywhere with the required connectivity.

Initial outlay costs for technology purchases are often prohibitive and, in order to remain on the cutting edge, the need to frequently invest substantial capital poses a tremendous challenge for many agencies, especially smaller departments. A shared or consolidated resource is an intriguing concept, and one that can result in significant cost savings to a law enforcement agency. By migrating to cloud-based platforms, public safety agencies will enjoy significantly lower equipment costs and will not be faced with the need to constantly spend money on the latest and greatest hardware and software.

Once the development team has completed the strategic plan, it should be reviewed and compared to the agency's vision and the department's mission statement for consistency. It should also be evaluated against any direction originally received from the executive management in order to ensure all relevant issues have been addressed.

It is now the job of the strategic plan coordinator to present the finished product—the agency's strategic plan—to key decision-makers for adoption. This will usually start with the department's executive management team and include the city council, board of supervisors or other oversight entities. After all key stakeholders agree to the plan, maximum dissemination of the agreed upon plan is extremely important. Although the published version of the strategic plan may be considered the "final" version, it is

important to remember that as a living document, the strategic plan is always subject to change, modification and refinement.

The establishment of an effective organizational vision will aid the department in determining how the organization should "look" as it implements its strategic plan. Many organizations may not be able to establish a firm organizational vision until after they have completed the planning process at least once. However, creation of such a vision is important for newly formed organizations, those lacking a previously implemented, effective strategic plan, those undergoing significant organizational restructuring, or a change in executive-level leadership.

c. The Implementation Process

The development of a strategic plan is only the beginning. Implementation is vitally important to avoid creating a body of work that does nothing more than sit on a shelf and become "credenza ware." It also damages the credibility of the department's leadership when a vision and plan are created and then to collect dust as their importance fades. Implementation includes establishing who is responsible for each action step that supports the parent strategy; who is responsible for administrative support and documentation of progress toward the department's goals; who monitors the plan for mid-course corrections and accountability; and, who polices the regularly occurring project reporting.

In order to measure the success of the strategic plan, it is necessary to set goals that have measurable objectives. An implementation schedule is an important component of the goal development process in order to provide guidance as to which goals should be implemented in which order.

d. Reassess and Refine

As important as the plan development, implementation and monitoring are, it is also necessary to assess implementation strategies for continued relevance and effectiveness. The strategic plan itself may remain relevant for only a few years and usually five at the most. The plan may be adjusted each year or more frequently to

address a changing operational environment. It should certainly go through the entire process discussed above every five years. Every aspect may not change with each new plan. For example, the department may choose to retain its mission statement and one or more relevant goals. Most parts of the plan, however, should see some adjustment or complete re-write to address contemporary issues that did not exist five years ago.

Examining trends and events and creating viable scenarios for the future will aid in the creation of a roadmap for moving toward a desirable future or away from an undesirable one. While futures study provides a glimpse into the distant future (10 years or more), strategic planning fills the gap between possible futures and the present. Agencies or entities cannot plan for the distant future while ignoring what is right around the corner, even if it means that the strategic plan serves no purpose other than to lay the foundation for these future events. However, strategic planning does more than that. It turns a vision into action and it provides a sense of purpose and focus for the organization.

3. Managing Change

In an effort to prepare our organizations for issues that will affect and change the ways in which we currently conduct business and to assist us in making good decisions towards these anticipated changes, we often imagine the future. The change created by an effective strategic plan may have little impact on existing processes, practices and personnel. On the other hand, the change could be so extensive that the upheaval it causes could derail or otherwise adversely impact the desired outcome. To prevent this, effective transition management must be consciously developed, implemented and managed to ensure the desirable outcomes do not destroy the agency in the process.

Managing change in an organization is often an underestimated or little understood stage in planning and implementation. Change management begins and ends with a presentation of the process to be implemented and training for those employees affected by it. Depending upon the complexity of the project or program, management of the transition should usually follow one of three models.

a. Developmental Change

Developmental change can be defined as normal process improvement of an existing program, function or condition. This systematic and logical change is usually readily accepted by the affected employees because it is within their comfort zone and area of expertise. Developmental change can be consciously initiated within the organization or it can be driven by external factors.

b. Transitional Change

Transitional change goes beyond improving existing processes, programs, functions or conditions. It is generally a complete replacement that is intended to solve a problem or exploit an opportunity. This transition is usually designed by a project team or at the direction of executive management. However, it can also be the result of external forces or influences that the organization must adapt to in order to thrive or survive. The program or condition that the organization is transitioning from must be physically and mentally abandoned or dismantled as the agency transitions to the new state of being. Coping with and adjusting to personnel issues during transitional change is a manageable task if the organization develops a thorough transitional change strategy.

c. Transformational Change

Anderson and Ackerman Anderson define transformational change as ." . . a radical shift from one state of being to another. . ."[48] The organization and its employees must change the way they define their agency and its mission or purpose. Because of the magnitude of transformational change, the outcome, and sometimes the process for getting there, are not always clearly defined or understood. The end result may not even resemble the outcome expected at the beginning of the transformation. There are plenty of examples of companies that did not see the need for transformational change as the market or business climate around them changed drastically. They either failed to change, or engaged in developmental or transitional change when transformational change was

[48] Dean Anderson and Linda Ackerman Anderson, *Beyond Change Management: Advanced Strategies for Today's Transformational Leaders* (San Francisco, CA: Jossey-Bass/Pfeiffer, 2001).

necessary. The misalignment of change models can occur when the organization is in denial about the level of change needed, or is unable to commit the energy and resources needed for transformational change. The end result is often a failed business enterprise or hostile take-over, or a governmental entity that ceases to exist or is forced to undergo transformational change in a less-than-friendly environment.

4. Commitment Planning

Change will not occur or will not be fully implemented without some level of buy-in or commitment from key stakeholders. Those responsible for implementing change can leave stakeholder commitment to luck or guesswork or they can plan methodically to assess the level of commitment and work to increase it to minimally acceptable levels where needed. Beckhard and Harris' commitment planning model charts the key stakeholders and displays their current level of commitment and the desired minimum level of commitment needed for successful implementation of change.[49] Levels of commitment are measured on a continuum ranging from a low of "No Commitment" through "Let It Happen" and "Help It Happen" to an ideal or high state of "Make It Happen."

Table 12 depicts the commitment-planning chart for managing the integration of emerging technologies into a public safety communications center.

[49] Richard Beckhard and Reuben T. Harris, *Organizational Transitions: Managing Complex Change* (Reading, MA: Addison Wesley Publishing Company, 1987).

Table 12. Commitment Planning Chart

Key Players	No Commitment	Let It Happen	Help It Happen	Make It Happen
Private Corporation				X
Dispatchers		X		
Dispatch supervisor		X		
Dispatch union		X		
Public Citizens			X	
State Coordinator			X	
911 Oversight Ofc				X
Agency Head				X
Chief Info. Officer				X
Patrol Officers		X		
City Council/Board of Supervisors		X		

Dispatchers and their union are included in the chart because they are the group most directly impacted by the change. Their work processes, job description and physical location of their employment may undergo a transformational change. Their support or acceptance will have the most direct impact upon the success or failure of the change being implemented. Public support from their union will drive support from its constituent members and contribute to a successful implementation.

Citizens attempting to access emergency services will benefit from the enhanced level of service they receive, but at the same time, several cities will see a loss in revenue because employees will be relocated to another area.

The oversight authorities in a given state, county or municipality must assist in implementing a very complex project for which there is no established roadmap or template for implementation. There will be pressure to succeed and to stay within budget, while maintaining the existing system during the transition. This will require personnel resources and continued funding, both of which are very limited.

The agency executive, board of supervisors and city council are motivated to support a positive transformational change in service delivery, but must balance that with competing budgetary issues. This type of project and the change it creates carries a high level of risk. Unsuccessful execution will be costly and demoralizing. Executive

management and political leaders must demonstrate a high level of support for the project to create and maintain momentum before and during the change.

The chief information officer and IT staff must manage a complex project for which there is no established roadmap or template for implementation. There will be pressure to succeed and to stay within budget. Maintaining the existing system during the transition will also require resources and continued funding. Lastly, the project team must manage customer expectations to ensure that the project scope does not become unmanageable. While the IT community does not need to believe in the change to implement it for the user community, lack of commitment can surely derail it before it reaches the customer.

Patrol officers will likely benefit from the end result, as dispatchers will not have to be responsible for answering radio traffic and emergency telephone calls at the same workstation. Currently, that is a major frustration for patrol officers. Frequently, upon contacting the dispatcher via the radio, officers are asked to wait until the dispatcher completes the 9-1-1 call he/she is handling. Officers will likely identify a negative aspect of the new model to be that dispatchers are not located in close geographic proximity to them. This will eliminate the opportunity to "put a face with a voice." Their acceptance of this transformational change will likely start in the "Let It Happen" category, however, it could likely improve to "Help It Happen" in a short period.

The private corporations who will design the new infrastructure stand to benefit from increased use of their systems as customer confidence. There will be concerns, however, with network capacity and increased operational costs due to their higher-end equipment capable of high-speed data transfers and multimedia applications. If this increased operational cost is passed on to the customer, in this case the agency, the corporations may experience a backlash of customer dissatisfaction. Corporations will also compete with their competitors for establishment of new standards for public safety computer-aided dispatch systems. Avoidance of proprietary data models will best position the industry to interface with public safety systems, however, the lure of capturing a large share of the market because consumers and government entities are locked into proprietary systems is tempting.

In most scenarios, a change of this magnitude will have been initiated by the agency head or chief information officer. Their buy-in or support is a given, unless a change in management occurs midway through the change implementation. To improve the likelihood of success a "critical mass" of individuals or groups should be identified and recruited.[50] Members of this group are chosen because they have the ability to carry others along with them or provide the leadership needed for other key players to follow. The pivotal groups in this change process are the dispatchers and their union. As the primary users of the communications center system, their acceptance or rejection of the change will carry great weight. The champions of this transformational change should identify informal leaders in the dispatcher ranks and work to win their support and find common goals with the union to ensure their continued advocacy for change.

Resistance from the two groups mentioned above should be mitigated by identifying concessions the organization can make to ensure buy-in. For example, a commitment to consolidating centers at a methodical pace, providing employees an opportunity to relocate, retire, transfer, or be retrained is imperative. Furthermore, examining what services should still be provided by the dispatchers can minimize concerns about a staggering increase in workload. In lieu of additional staff, automated processes for performing similar functions can be included in the bid specifications. In this way, a case can be made that the volume of calls or dispatcher workload should not increase (or increase minimally) as a ratio to the volume of calls each dispatcher must answer during a given period.

All stakeholders, both internally and externally, must know the department's progress during the implementation process. The leaders in the organization will have to be aware of change resistance. This could be from internal and external stakeholders. If left untreated, resistance has the ability to sabotage the entire strategic plan. Strong communication will build employee knowledge and ultimately, trust. That trust will prove invaluable, especially when change needs to occur. Everyone will be tasked to drive the implementation towards success, especially members of the management team.

[50] Beckhard and Harris, *Organizational Transitions: Managing Complex Change*.

Lastly, transparency will be stressed to every opportunity in order to emphasize the importance of trust within each relationship.

The stakeholders depicted in Table 13 are those known prior to implementation. The list may grow or shrink as the change process moves forward.

Table 13. List of Key Stakeholders

Stakeholder
Agency Director
Chief Info. Officer
Management Staff
Patrol Officers
Project Manager
Project Team
Dispatchers
Dispatch supervisor
Dispatch union
Public Citizens
State Coordinator
911 Oversight Office

C. EVALUATION

Oftentimes, IT projects include some form of evaluative process. An effective and meaningful evaluation tool will help document the success or failure of the major outcomes of the strategic planning and change management processes. Planned and unplanned events occasionally generate an after-action report for use in documenting lessons learned and to assist with future planning efforts.

An outcome evaluation process will provide a template for identifying success criteria or objectives, measures, an evaluation methodology and actionable conclusions. Initial activities most likely will not be a part of the outcome evaluation process. These activities are inputs that served as the catalyst for the goals and objectives and transition activities. There would be nothing to measure without these initial planning activities. Those efforts are typically already documented in feasibility studies, project charters, and

project plans. The outcome evaluation should focus on the output of those initial efforts and measure their success.

The strategic plan objectives in Table 14 will be measured in the outcome evaluation.

Table 14. Strategic Plan Outcome Objectives

Objective	Measure	Responsible Party or Entity
Determine a funding mechanism for the deliverables that require capital outlay.	• Are grant funds available for the life of the project? • Are special funding sources available and are they being utilized to their fullest extent? • Has the oversight office received capital outlay approval from Finance Department	Fiscal Management, Project Manager Fiscal Management, Project Manager Oversight Office, Fiscal Management
Locate or design cloud-based technology that will support the new communications center model	• Are on-going maintenance and upgrade costs included in the baseline budget? • Are annual software licensing costs less than or equal to 15% of the purchase price? • Have maintenance and operations costs been added to the appropriate budget baseline?	Procurement Team Procurement Team Procurement Team
Evaluate the current dispatch model and determine key changes in workload and service delivery model	• Does the new service model optimize the use of new technology? • Are there certain functions that will be added/removed from the Dispatcher job description?	Project Manager Employee Relations, Union representatives
Develop an educational campaign for employees to learn about the new model and	• Are employees aware of how much better the level of service to the public will be?	Chief, Chief Information Officer, selected

Objective	Measure	Responsible Party or Entity
why we are migrating to cloud-based technologies.	• Are employees aware of how much long-term funding this project will save and how that savings will benefit them? • Are employees aware of their options regarding relocation, transfer, reassignment, or retraining?	dispatchers, Union representatives Management Staff, Chief Information Officer Union representatives

Outcome evaluations will occur at identified milestones for some objectives and after the completion of the strategic planning goal or project for others. Outcomes evaluated at identified milestones will allow for correction and adjustment while the project is still in progress. Those evaluated after the goal or project is completed will provide performance feedback and a planning template for future projects or planning goals.

Executing a change of this magnitude would be quite risky and will be seen as dramatic, no matter what role individuals play within the organization. Specifically, the impact on communications centers, patrol operations and the culture of the agency will be significant. This transformational change will only be successful if those stakeholders responsible for project success and successful implementation of the strategic planning goals understand and implement appropriate change management practices.

Transition management cannot begin and end with project management, training and public education. An understanding and acknowledgment of the appropriate change model, establishment of a commitment-planning model, well structured and executed implementation and evaluation are all necessary for effective transition management. Without these elements, an important step in strategic plan implementation will be missed. This step can make or break the strategic plan and possibly the department.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SUMMARY

Although the technology associated with reliably and rapidly transmitting voice and data traffic from one point to another has been around for years, the mechanism in which those tasks can be accomplished has improved exponentially and most recently, with the advent of cloud-based technology, surged into the virtual world. Public safety dispatchers can have all necessary information at their fingertips through the use of emerging technological advancements, such as interactive GIS mapping applications, GPS location data and RoIP. That same dispatcher could answer a call for service from the public, summon emergency response personnel or other service providers, such as tow trucks or taxis, determine the location of all patrol units and dispatch the closest available unit from any computer where an Internet connection exists. Finally, picture all of those technologies working seamlessly across a virtual network, using the latest hardware and with software and security updates being constantly applied in an off-site data center with unlimited capacity.

Public safety agencies that have more than one communications center could embark upon consolidation efforts, essentially eliminating the need for multiple standalone facilities. Depending on the size and scale of the organization, they could downsize to a single center or just a few. Furthermore, for those that choose to keep more than one, managers would have the ability to reroute dispatch traffic to a different center, in the event of an emergency or when the volume has exceeded the capacity of their respective center.

Nearly all of the technologies mentioned above already exist. What is missing is the implementation of some of the ideas and the confluence of a few key trends and events to drive the implementation and adoption of the rest. The future model of law enforcement communications centers is on the verge of a paradigm shift, which will vastly change the way dispatching services are provided. It is imperative that agency executives understand the long-term benefits of emerging technologies and prepare for

their incorporation into future planning models. They must also recognize that delays on their part will incur unnecessary expenditures of time and money.

Incorporating these emerging technologies will certainly have an impact on communications centers, patrol operations and the culture of an agency. This transformational change will only be successful if those responsible for the project's success and successful implementation of the strategic planning goals understand and implement appropriate change management practices. Change will not occur or will not be fully implemented without some level of buy-in or commitment from key stakeholders. As the primary users of the communications center system, the dispatchers' acceptance or rejection of the change will carry great weight.

B. RECOMMENDATIONS

It is imperative that public safety agencies begin preparing for emerging technologies and evaluate the current of their public safety communications centers to determine their readiness for what is on the horizon. Similarly, if agencies have not established a strategic vision or plan to prepare themselves for the next five to ten years, they should begin immediately. There are too many variables to work "on-the-fly."

Without some advance planning and the implementation of a cloud-based platform, a public safety communications center faced with a spontaneous evacuation could seamlessly move its operation to an adjoining dispatch center. With an NG9-1-1 network, the calls could be re-routed to another PSAP or multiple PSAPs within minutes. Depending upon the status of the other PSAPs, the dispatch center personnel could physically go to another PSAP to assist in accepting and dispatching their own calls for service, or respond to a backup location and resume call taking and dispatching there.

In an NG9-1-1 network, this transition is easier and more dynamic than the existing E911 configuration. Any PSAP connected to the NG9-1-1 network, if allowed, could be capable of receiving calls for another. This means that if the entire region were compromised, there could still be potential call routing options. As an additional layer of redundancy, some of the NG9-1-1 network vendors offer nation-wide call centers, which could be utilized as a last resort. Furthermore, if radio and CAD functionality are cloud-

based, those facets could also be re-routed and the public would not experience any type of disruption.

C. OPPORTUNITIES FOR FUTURE RESEARCH

These technological advancements bring a myriad of new opportunities and challenges, however, this thesis was not able to cover every aspect. One key facet that warrants additional thought is the impact of communications center consolidation on personnel. For example, if several entities consolidate into one conglomerate, how will this impact the dispatchers? The creation of a new location to house all of them may be feasible and may improve efficiency; however, it may come with a negative impact to their established culture. Similarly, the use of supervisors and managers from various agencies to supervise subordinates from different departments may pose challenges. Perhaps consolidated communications centers should maintain independent supervisors and managers, with the personnel simply being co-located. The facility could have one "manager" of the facility, who does not have functional supervision of the dispatchers? Along the same lines, should the communications center be operated under a Joint Powers Authority agreement? If not, who is responsible for making decisions on behalf of the dispatch center? Do all employees, regardless of employing agency, follow the same set of rules?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. TREND LISTING

The following is a complete list of the trends identified by the Nominal Group Technique panelists.

1. State of the economy
2. Consolidation and regionalization
3. Availability of resources
4. Standardizations of operational procedures
5. Standardization of technologies
6. Availability of cloud resources
7. Reliability of cloud
8. Reliability of WAN
9. Public expectation
10. Level of education (KSAs), training
11. Outsourcing to elsewhere (Flatworld 3.0)
12. Security with cloud form
13. Homeland security concerns
14. Integrated command and control
15. Political ramifications
16. Government control
17. Technology convergences (inoperability)
18. Acceptance of VoIP
19. Human interaction
20. Home network reliability
21. Advancement of wireless technologies
22. Mobility
23. Management oversight
24. Change management
25. Virtualization
26. Availability of fiscal resources

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. EVENT LISTING

The following is a complete list of the events identified by the Nominal Group Technique panelists.

1. Budget cuts
2. Rolling blackouts
3. Unfunded mandates
4. Hiring freezes
5. Bankruptcy of governments
6. Natural disasters
7. Targeted network outage
8. Water shortage
9. Terrorist threat level
10. Legislation mandates
11. Technological changes
12. Forced consolidation for small entities
13. Terrorist attack
14. Internet virus
15. An elimination of grant funding
16. Decision to outsource/privatization
17. Catastrophic service interruption
18. Implementation of NG9-1-1
19. Change in government political leadership
20. Consolidation of government agencies
21. Elimination of state services
22. Competing for contracts
23. Breach of personal and private information
24. Pandemic

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alston, Farnum, and John Bryson. *Creating and Implementing Your Strategic Plan—A Workbook for Public and Nonprofit Organizations*. San Francisco, CA: Jossey-Bass, 2005.

Anderson, Dean, and Linda Ackerman Anderson. *Beyond Change Management: Advanced Strategies for Today's Transformational Leaders*. San Francisco, CA: Jossey-Bass/Pfeiffer, 2001.

Archbell, Ian. "Use the Cloud to Lower Sky-High Costs." *Law Enforcement Technology Magazine*, March 2011.

Bardach, Eugene. *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*. Thousand Oaks, CA: CQ Press, 2012.

Beckhard, Richard, and Reuben T. Harris. *Organizational Transitions: Managing Complex Change*. Reading, MA: Addison Wesley Publishing Company, 1987.

Bishop, Peter, and Andy Hines. *Thinking About the Future, Guidelines for Strategic Foresight*. Washington, DC: Social Technologies, LLC, 2006. ISBN-13: 978–0-9789317-0-4.

Business Insider. "NSA: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them." Accessed March 22, 2014. http://www.business insider.com/how-many-docs-did-snowden-take-2013-12.

California Office of the Chief Information Officer. "California 9-1-1 Strategic Plan." July 30, 2010. http://www.cta.ca.gov/PSCO/911/pdf/911_Strategic_Plan.pdf.

Cornish, Edward. *Futuring—The Exploration of the Future. World Future Society*. Bethesda, MD: World Future Society, 2004. ISBN 0–930242-61-0.

Coutinho, Ryan. "Cloud Computing or Cloudy Computing." *Public Management*, April 2012.

Dargha, Ramkumar. "Cloud Computing: From Hype to Reality. Fast Tracking Cloud Adoption." Presented at the International Conference on Advances in Computing, Communications and Informatics, Chennai, T Nadu, India, August 3–5, 2012.

Delp, Peter, Arne Thesen, Juzar Motiwalla, and Neelakantan Seshardi. *System Tools for Project Planning*. Bloomington, IN: International Development Institute, 1977.

European Network and Information Security Agency. *Cloud Computing; Benefits, Risks, and Recommendations for Information Security*. Crete, Greece: 2009.

———. *Security and Resilience in Governmental Clouds*. Crete, Greece, 2011.

Federal Communications Commission. “PSAP Registry.” January 4, 2013. http://transition.fcc.gov/pshs/services/911-services/enhanced911/psap registry.html.

Federal Computer Week. “When the Cloud Makes Sense.” 2011. http://fcw.com/ DownloadingCloudComputing.

Fischer, Eric A., and Patricia Moloney Figliola. *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management*. CRS Report R42887. Washington, DC: Library of Congress, Congressional Research Service, January 4, 2013.

Garrison, Gary, Sanghyun Kim, and Robin Wakefield. “Success Factors for Deploying Cloud Computing.” *Communications of the ACM* 55, no. 9 (September 2012).

Gilmore Commission Report. *Forging America’s New Normalcy: Securing Our Homeland Preserving Our Security*, vol. Five. Arlington, VA: RAND Corporation, December 15, 2003.

Google. “Security.” Accessed January 18, 2013. http://www.google.com/enterprise/apps/ government/benefits.html?section=security.

Gordon, Theodore. “Cross-Impact Method.” *AC/UNU Millennium Project*, 1994.

Higgins, John. “Feds Aim to Lock Down the Cloud.” *Technology News World*, December 13, 2011. http://www.technewsworld.com/story/73956.html.

Kundra, Vivek. *25 Point Implementation Plan to Reform Federal IT Management*. Washington, DC: U.S. Government Printing Office, December 2010.

OWASP. “Cloud Top 10 Security Risks.” Last modified January 23, 2014. https://www.owasp.org/index.php/Category:OWASP_Cloud_-_10_Project.

Panzarion, Matthew. “Apple’s Tim Cook Says There Are Now Over 100M iCloud Users, Marking 15M User Growth in 21 Days.” February 14, 2012. http://thenextweb. com/apple/2012/02/14/apples-tim-cook-announces-that-there-are-now-over-100m-icloud-users-marking-15m-user-growth-in-21-days.

Ruiz-Alvarez, Arkaitz, and Marty Humphrey. “A Model and Decision Procedure for Data Storage in Cloud Computing.” *IEEE Computer Society*, 2012.

Smith, Andy. “Derecho 911 Problems Lead to Changes from Verizon, Arlington County (#DMVReads).” *The Washington Post—Blogs*, August 20, 2012. http://www.washingtonpost.com/blogs/the-buzz/post/derecho-911-problems-lead-to-changes-from-verizon-arlington-county-dmvreads/2012/08/20/eecb31b2-eade-11e1-b811-09036bcb182b_blog.html.

Thor, Olavsrud. Security in the Cloud Is All About Visibility and Control. *Network World*, February 17, 2012. http://www.networkworld.com/research/2012/021812-security-in-the-cloud-is-256332.html?page=3.

U.S. Department of Commerce. National Institute of Science and Technology. *The NIST Definition of Cloud Computing*, September 2011.

U.S. General Services Administration. “About FedRAMP.” Last reviewed March 25, 2014. http://www.gsa.gov/portal/category/102375.

Vision Center for Futures Creation, The. “Trend Analysis.” Accessed January 10, 2014. http:/www.framtidsbygget.se/E/trendanalys/index.htm.

White House. *25 Point Implementation Plan to Reform Federal Information Technology*. Washington, DC: White House, December 9, 2010.

Wikipedia, s.v. “Cloud Computing.” Last modified November 17, 2012. http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=523482934.

———. “Federal Information Security Management Act of 2002.” Accessed November 17, 2012. http://en.wikipedia.org/w/index.php?title=Federal_Information_Security_Management_Act_of_2002&oldid=480447665.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California